InstantKey
User Manual

L7 Networks
Secure Networks at Layer-7

Copyright

Trademarks

Technical Support

This manual provides you a detailed installation & setup guide of the product. You can also download the documents from our website at http://www.l7-networks.com/L7_2005/products.download.html .

If you have any technical problems or suggestions, please contact our technical support center. Please prepare the following information to save the time when communicating.

- Product model & serial number, where you can get it from CLI command: “sys ver”.
- Purchasing time & maintainence contract
- When you get this product
- Briefly describe the problems & the steps you have already tried.

Contact / Location	Email	Telephone	Address
Taipei	service@L7-Networks.com	+886-2-27936053	3F NO.289 Sinhu 3rd Rd. Neihu District, Taipei City 11494, Taiwan
Hsinchu	service@L7-Networks.com	+886-3-666-8896	10F NO.25 MinZu Rd. Hsinchu, Taiwan
Shanghai	service@L7-Networks.com	+86-21-5434-9678	L7 Networks Inc. (R&D Shanghai office)
Beijing	service@L7-Networks.com	+86-21-5434-9678	Alphasolutions Co., Ltd.
Singapore Indonesia	service@L7-Networks.com	+65-31503660	L7 Networks Inc.
Thailand	service@L7-Networks.com	+1-408-844-8850 +1-408-844-8841	Solution One Ltd.

Remote support: Launch your SSLVPN client (tunnel.exe) which has already accompanied with the management server software. Select a tunnel for our support team to connect to your live place to solve the problem for you. Or you can use TeamViewer to setup a remote desktop for us to do the troubleshooting for you.

About This Manual

This manual use the web-based user interface (WBI） of the product to describe how to setup the product. In order to help you how to use the product, you must understand the how to use WBI.

Who should read this manual?

This manual teaches you the detailed configuration of the product. Any one who are responsible to setup, monitor, decide the content policy, or receive the report, should read this manual

Related Documents

- Product CD

  Refer to the documents inside the CD.
- Quick Installation Guide (QIG)

  QIG can assit you to quickly install the hardware and software.
- Online support

  Online support gives you MSN / Skype & SSLVPN connectivity that allows our support team to contact you and to see your desktop without opening your firewall settings.
- Web site support

  Refer to the website information, including the most updated firmware / pattern release note, or the most upcoming features that will be release in the future.

Contact

The methodologies provided in this manual has already been tested and verifed. If you have found any functions that has already been modified in the software / hardware, please email your suggested directions to our support email address: service@l7-networks.com

You can use email address to tell us your messages. If you want to subscribe our e-paper, you can also email your address to the following email address:

service@L7-Networks.com

You can visit our website to search for any advanced progress of this manual or information:

http://www.L7-Networks.com

Table of Contents

Part 1

Overview

New Release 5.0.01

Chapter 1
Product Overview

This chapter briefly introduces to you how to quickly install the product

What are employees doing at work?

Employees often use Outlook to receive emails, Internet Explorer to browse websites, Instant Messengers (IM) such as MSN/Skype to chat with friends, and P2P software such as BT / eDonkey / Xunlei / KaZaA / Kuro / ezPeer to download illegal data. Among them, Email and IM are the channel for information leakage or virus intrusion, while P2Ps are the bandwidth killers and may contain many spyware. What is worse, IM wastes employee's productivity by friends' interrupt during the office hours. However, IM can save communication cost and even make communications more efficient so that many enterprises are willing to allow IM.

Tough IM/P2P: Tunneling Through Firewall

Enterprises that emphasize network security may have deployed Email/Web auditing / management systems. In comparison, IM and P2P lack the auditing/recording/behavior management/content management/bandwidth management because IM/P2P software are optimized to tunnel through Firewalls. MSN / Yahoo / ICQ / AOL / Skype / Google Talk can tunnel themselves to behave like Web/ Email to cheat Firewalls, tunnel through proxy servers, or even encrypt themselves. Network administrators cannot manage them completely.

1.1 Packing

Please check your packing and make sure you have the following accessories. If you have questions, please ask your local dealers.

No.	Name	Quantity	Notes
1.	device	1	
2.	L-shape chassis locker	2	
3.	screw	6	
4.	RJ-45 network cable	1	
5.	AC power cable	1	
6.	RS-232 console cable	1	
7.	CD	1	

FIGURE 1-1 Items included in the package

1.2 Hardware Installation

The product can be locked onto a standard 19-inch chassis or placed on any Figures. Please use the screws inside the packing to lock the L-shape lockers with the device. Finally, lock the device to the chassis.

Please check if the following network equipments are ready or not:

1. **Device**
2. **Swich/Hub**
3. **Desktop or notebook PC with copper network interface**

1.3 Wiring

1. **Power:** Connect the power to the power socket and turn on the power switch.
2. **Console:** Use RS-232 console cable to wire between the console port and the desktop PC. Set up the HyperTerminal of your PC into 115200, N, 8, 1 and no hardware flow control.
3. **MGMT Interface:** the management interface is used for uploading configuration or accepts logs from the device. The management server must be in the same subnet of the management interface.
4. **Internal Interface:** this interface connects to the internal network switch at your LAN side.
5. **External Interface:** this interface connects to the external network device, such as ADSL modem or router / firewall at your WAN side.
6. **HA Interface:** this interface connects to another same product to provide high availability function so as to make sure that the function will still work even hardware failure occurs.

1.4 System Defaults & Examples

In the following Figure you can lookup the default value of the device. Remember the the INT & EXT interfaces do not need any IP address when they are operating in bridge mode. The order of each interface in different models is different. When you first use the product, enter the CLI to check the order of the interfaces. In priviledge mode, enter “ip show” to lookup the numbering of the interface and the function of the interface.

Items		Default	Example
Password		admin	admin
Internal	Port No.	1	N/A
	IP Address	N/A	N/A
	Subnet mask	N/A	N/A
	Status	DOWN	UP
External	Port No.	2	N/A
	IP Address	N/A	N/A
	Netmask	N/A	N/A
	Status	DOWN	N/A
MGT	Port No.	3	3
	IP Address	192.168.1.1	192.168.168.201
	Netmask	255.255.255.0	255.255.255.0
	Gateway IP	192.168.1.254	192.168.168.254
	Primary DNS	0.0.0.0	168.95.1.1
	Secondary DNS	0.0.0.0	0.0.0.0
	Status	DOWN	UP
HA	Port No.	4	4
	IP Address	N/A	N/A
	Netmask	N/A	N/A
	Status	DOWN	DOWN
Management Server	IP Address	Undefined	10.1.1.10
	Subnet mask	Undefined	255.255.255.0
	Gateway IP	Undefined	10.1.1.254
	Primary DNS	Undefined	168.95.1.1
	Secondary DNS	Undefined	N/A

FIGURE 1-2 Related System Defaults

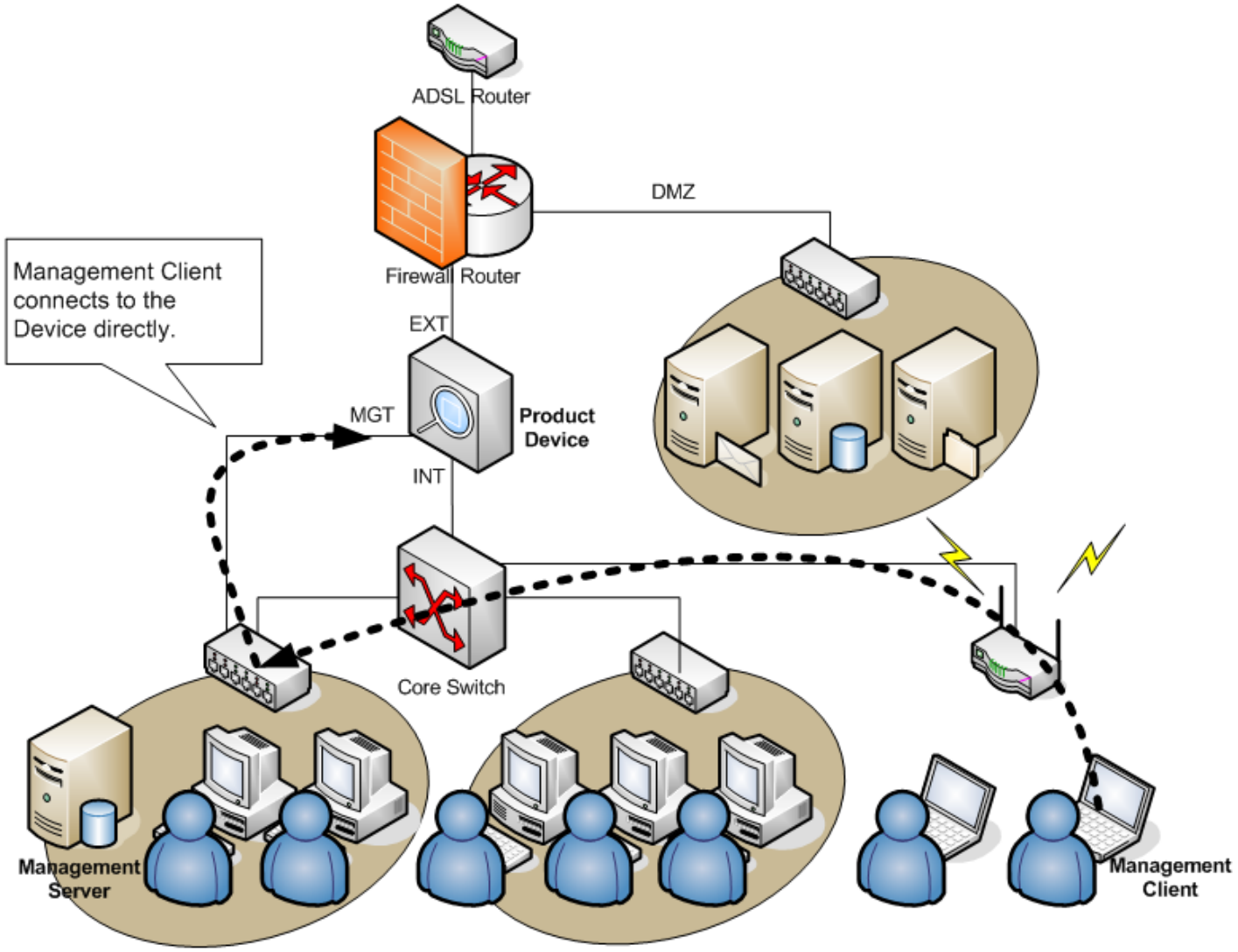


FIGURE 1-3 2-Tier Architecture

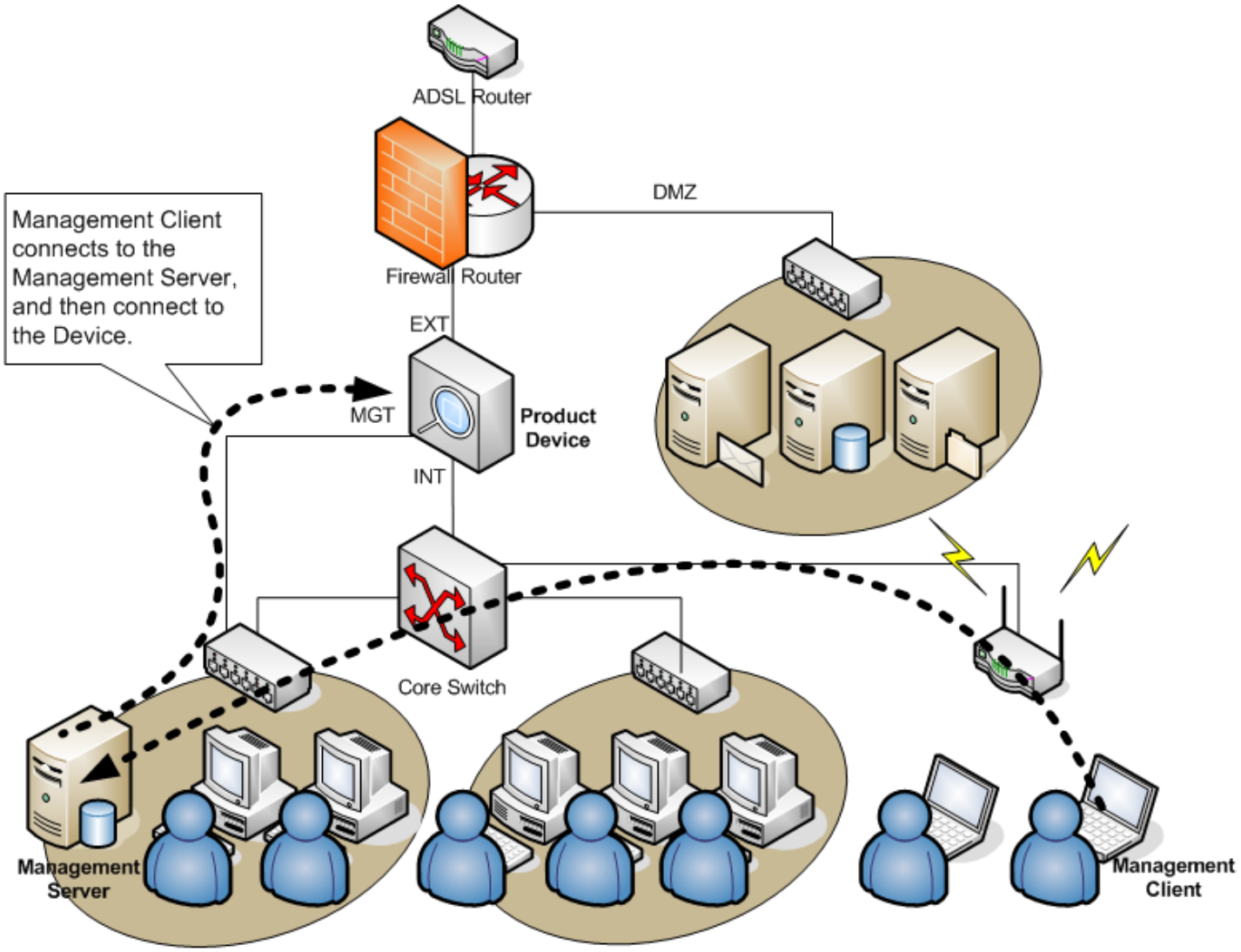
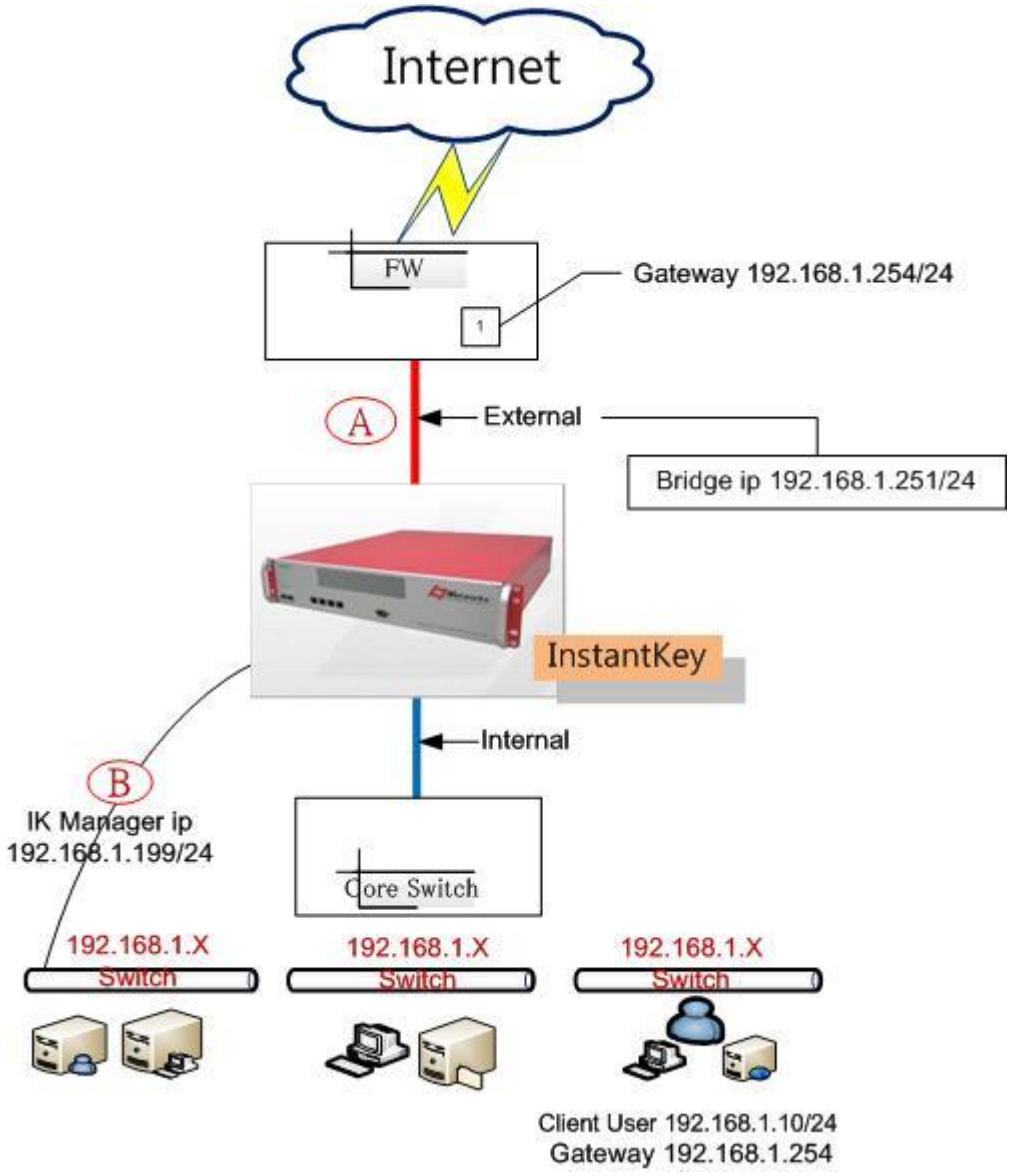


FIGURE 1-3 3-Tier Architecture

1.5 Setup IP & Routes

1.5.1 Users are in the same networks as Firewall LAN

If users are in the same network as Firewall LAN interface, the situation is the simplest. PCs' gateway are assigned to the Firewall's LAN interface, for example 192.168.1.254.



The device is connected between the core switch and the firewall. Label A indicates that the bridge IP should be set in the network of the Firewall-Switch segment, say 192.168.1.251.

Label B in the figure indicates the management IP of the device, say 192.168.1.199. Note that HTTPS traffic will still use its original IP to connect to the HTTPS server in stead of using the bridge IP. However, the system requires to lookup DNS through the management port.

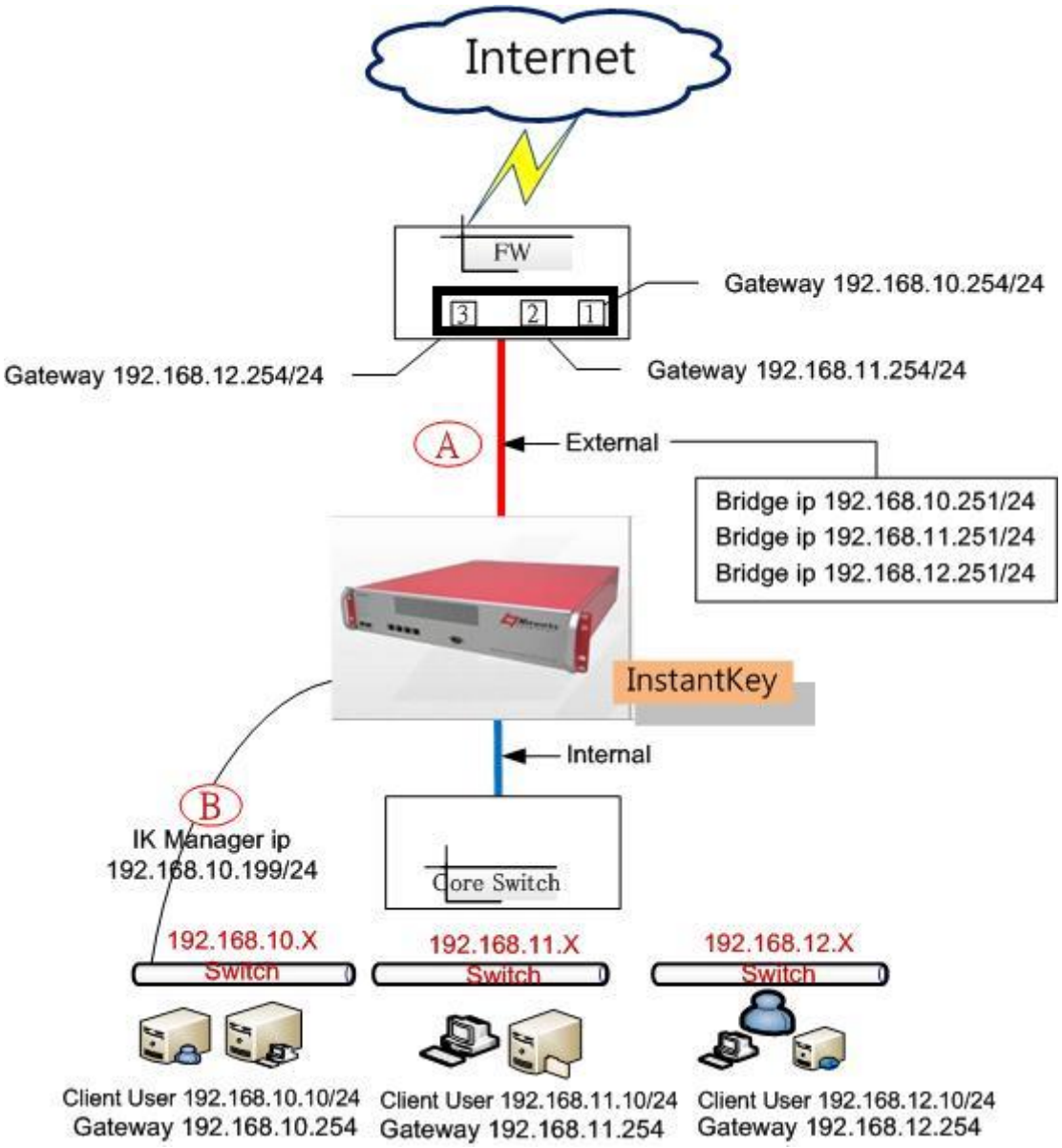
1.5.2 Users are in the same networks as Firewall LAN (Multiple Subnets)

If users are in the same network as Firewall LAN interface, but the interface is binded with multiple IPs for multiple subnets, say 192.168.10.254, 192.168.11.254, and 192.168.12.254. Only one physical port of the Firewall's LAN interface is logically segmented into three subnets..

The device is connected between the core switch and the firewall. Label A indicates that the bridge IP should be set in the network of the Firewall-Switch segment with multiple IP addresses, say 192.168.10.251, 192.168.11.251, and

192.168.12.251. And these three bridge IPs should be assigned with three different gateways, say 192.168.10.254, 192.168.11.254, and 192.168.12.254.

Label B in the figure indicates the management IP of the device, say 192.168.10.199. Note that HTTPS traffic will still use its original IP to connect to the HTTPS server in stead of using the bridge IP. However, the system requires to lookup DNS through the management port.

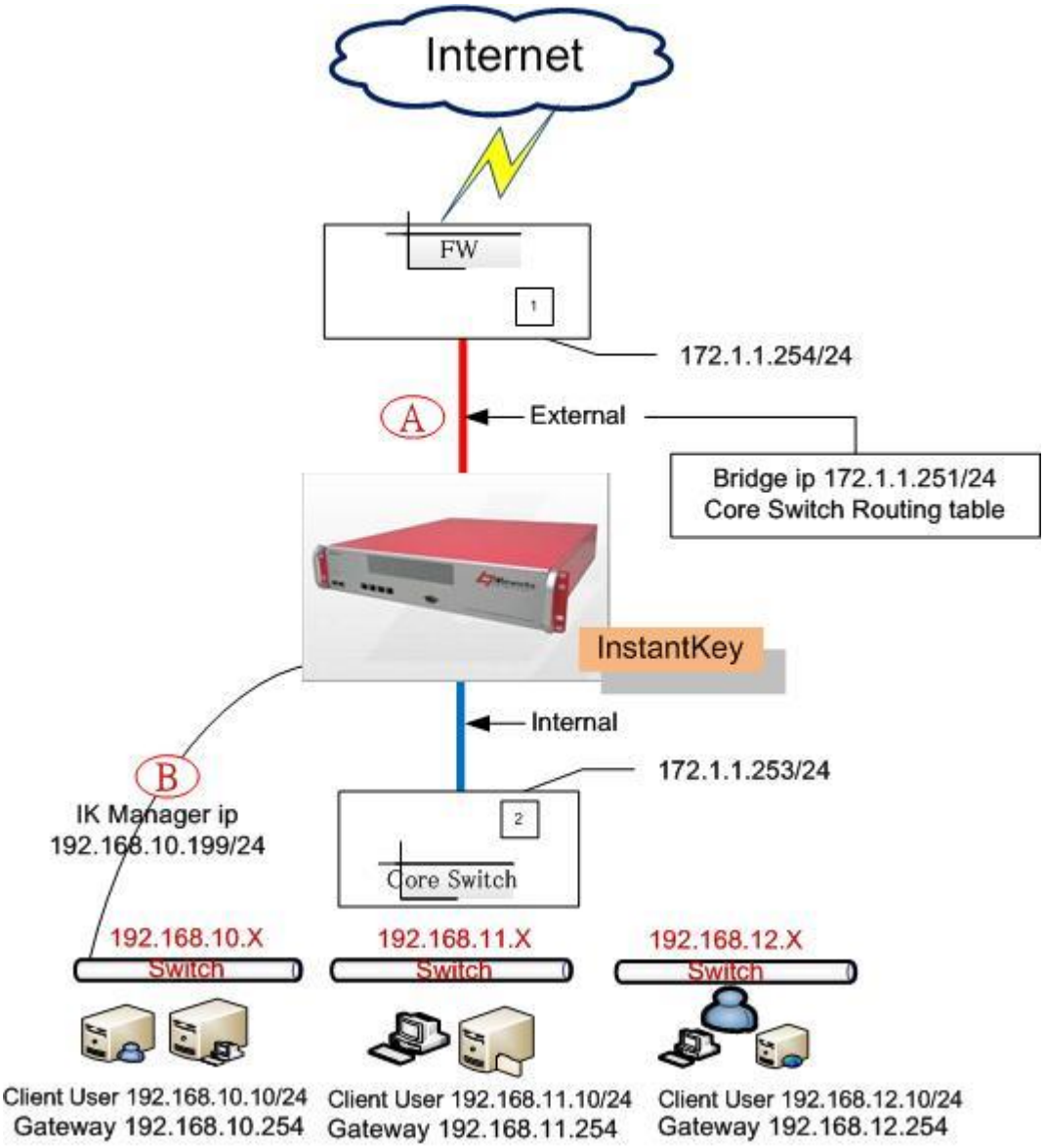


1.5.3 Users are NOT in the same networks as Firewall LAN

If users are NOT in the same network as Firewall LAN interface, we are required to configure routing for the SSL proxy to know the internal subnet and the internal gateway so as to forward the HTTPS response back to the correct client PC..

The device is connected between the core switch and the firewall. Label A indicates that the bridge IP should be set in the network of the Firewall-Switch segment, say 172.1.1.251 with gateway set to 172.1.1.254. However, the SSL proxy needs to know there are 192.168.10.X, 192.168.11.X, and 192.168.12.X subnets are below the L3 core switch 172.1.1.253. So you need to configure three routing rules for the device as [192.168.10.0/24 172.1.1.253] and [192.168.11.0/24 172.1.1.253] and [192.168.12.0/24 172.1.1.253].

Label B in the figure indicates the management IP of the device, say 192.168.10.199. Note that HTTPS traffic will still use its original IP to connect to the HTTPS server in stead of using the bridge IP. However, the system requires to lookup DNS through the management port.



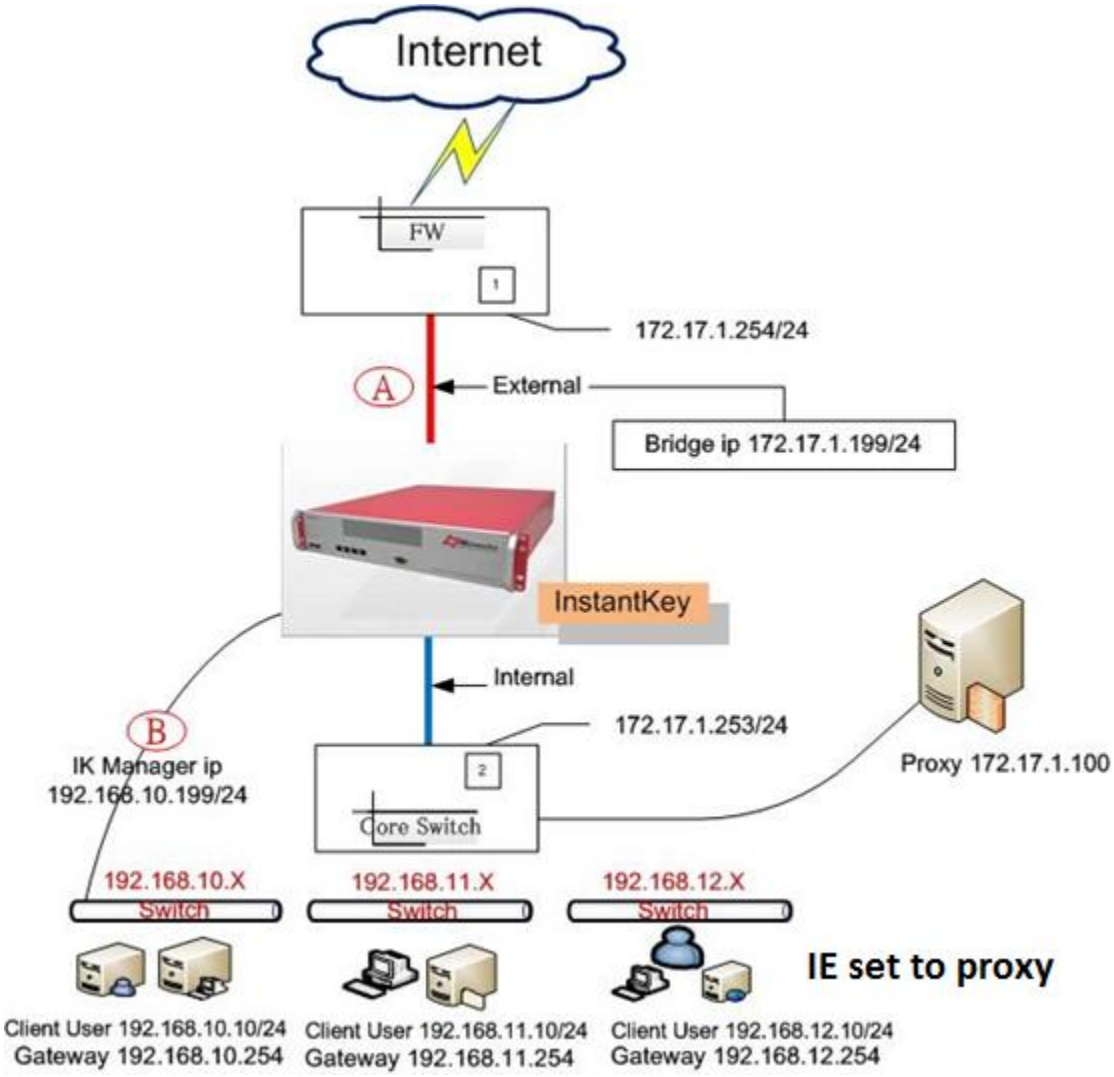
1.5.4 Users connects to internal proxy first

If users are configured to use proxy to go to the Internet, and the firewall limits that only the proxy IP 172.17.1.100 can go to the Internet, we usually configure the deivce also in proxy mode to intercept SSL connections.

The device can sit as a standalone proxy (only INT1 interface is needed to be connected) or be connected between the core switch and the firewall. In the latter case, Label A indicates that the bridge IP should be set in the network of the Firewall-Switch segment, say 172.17.1.199 with gateway set to 172.1.1.254. However, the SSL proxy needs to know there are 192.168.10.X, 192.168.11.X, and 192.168.12.X subnets are below the L3 core switch 172.1.1.253. So you need to configure three routing rules for the device as [192.168.10.0/24 172.1.1.253] and [192.168.11.0/24 172.1.1.253] and [192.168.12.0/24 172.1.1.253].

Label B in the figure indicates the management IP of the device, say 192.168.10.199. Note that HTTPS traffic will still use its original IP to connect to the HTTPS server in stead of using the bridge IP. However, the system requires to lookup DNS through the management port.

In proxy mode, users are required to manually assign https proxy server to **172.17.1.199:3129**. This can also be done by using Active Directory settings to force all users to have such settings. The device will use the IP 172.17.1.199 to go to the Internet. The Firewall should allow 172.17.1.199 to go out to outside port 443 servers. If needed, port 53 should also be opened for that IP.



Chapter 2
2-tier Architecture

This chapter introduce to you how to install the management server software to control the system

2.1 Installing Management Client

2.1.1 Requirements

- ✓ Operatiing System must be at least Windows 2000/2003 or Windows XP. If your operating system is in English version, please install your preferred language pack. For example, the Chinese Traditional language pack is prompted when you are installing the management server. Click the Install button to start installation.

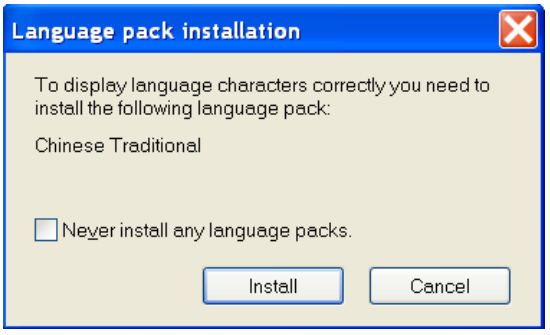


FIGURE 2-1 Language pack installation screen

- ✓ Hard disk space: at least 80GB available space, but we strongly suggest to have 120GB available space.
- ✓ CPU: at least Pentium 4.
- ✓ Memory: at least 256MB but we strongly suggest to at least have 512MB.
- ✓ If your operating system is Windows XP service pack 2 with built-in Firewall enabled, you must follow the steps below to open the ports: UDP/514, TCP/1080, and TCP/3306. In this way, all packets from or to the management server will not be blocked.
  1. Go to Start > Settings > Network Connection.
  2. Right click the Local Area Network and select Content.
  3. Go to Advance > Settings > Exception and click the Connection Ports...
  4. Enter the name and the port number to allow the following network ports.

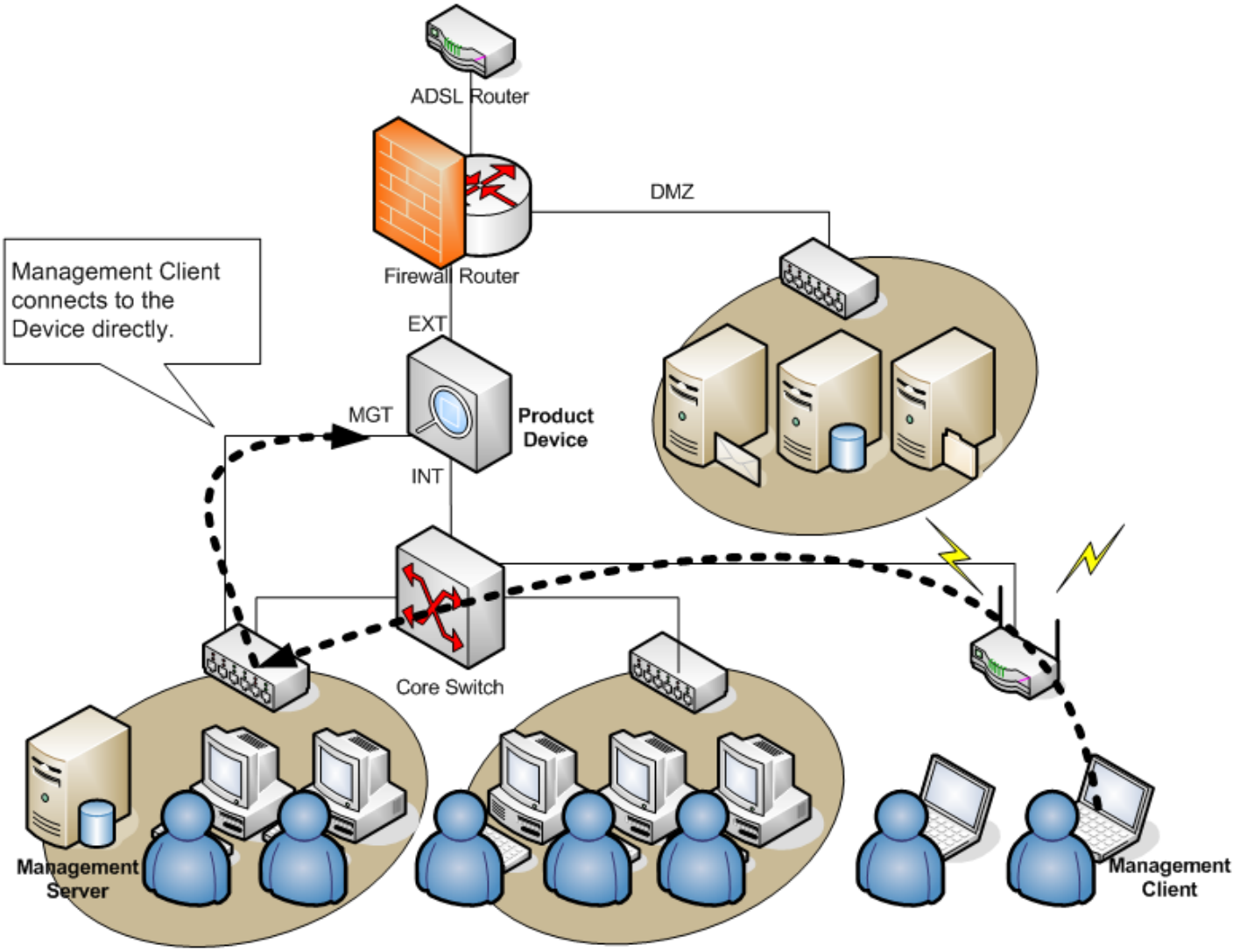
Name	Port Number	Protocol
Log Server	514	UDP
Socks	1080	TCP
Database Server	3306	TCP
HTTP Server	80	TCP

FIGURE 2-1 Firewall settings of management server

2.1.2 Procedures

1. Install the Management Server
2. Install the AD Log Server
3. Upgraing the Management Server
4. Browsing the CD

5. Uninstall Management Server



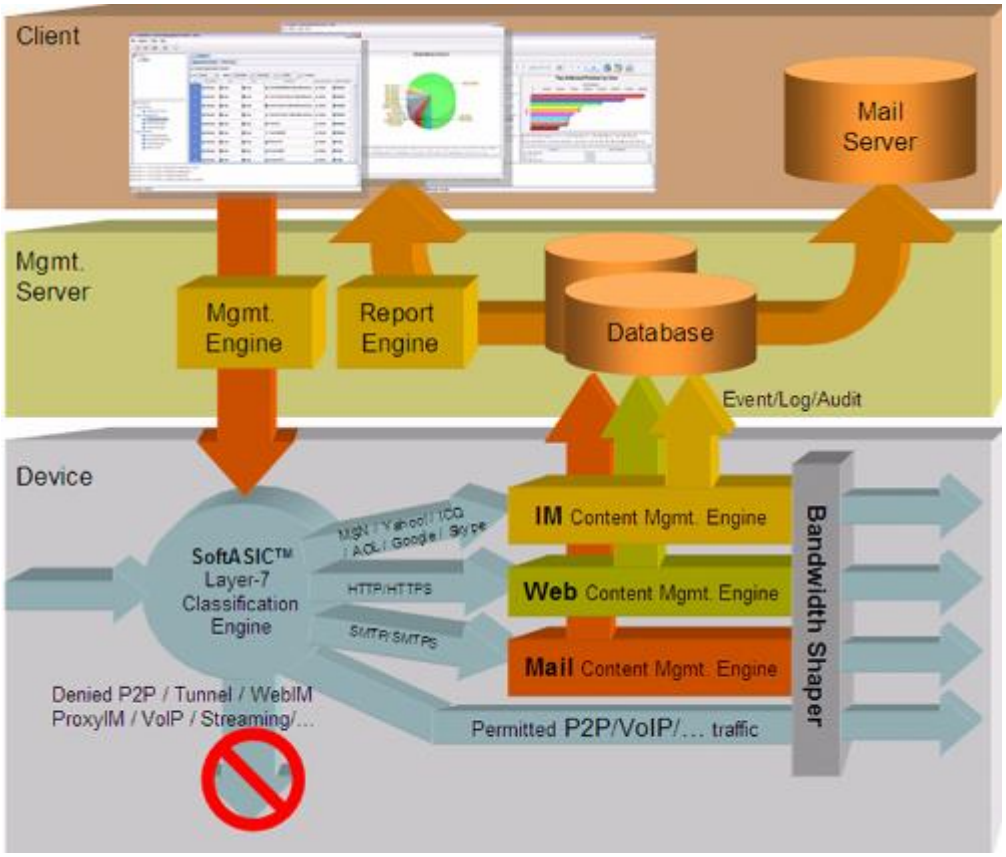
Chapter 3
3-tier Architecture

This chapter introduce to you how to install the management server software to control the system

3.1 What is 3-tier Architecture?

3-Tier Architecture: Maximize the Performance, Availability, and Functionality

Layer-7 network eqipments often do computing-extensive tasks and require better architecture to maximize the performance, availability, and functionality. The product incorporates the 3-tier architecture to boost the performance for every purpose.



1. **Tier-1: Device**: The device should aim at rapidly and accurately doing content inspection. In such a way, the device which is installed inline at the network will not influence the network performance.
2. **Tier-2: Management Server**: The management server takes the responsibility to centralize the management to multiple devices, while accepting event logs into database for further reporting & analysis.
3. **Tier-3: Management Client**: The management client can be any PC with a java-enabled browser. As long as he/she can connect to the management server, he/she can control all the devices under the server.

3.2 Installing Management Server

3.2.1 Requirements

- ✓ Operatiing System must be at least Windows 2000/2003 or Windows XP. If your operating system is in English version, please install your preferred language pack. For example, the Chinese Traditional language pack is prompted when you are installing the management server. Click the Install button to start installation.

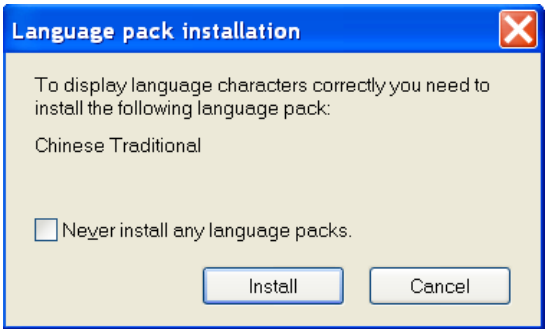


FIGURE 3-1 Language pack installation screen

- ✓ Hard disk space: at least 80GB available space, but we strongly suggest to have 120GB available space.
- ✓ CPU: at least Pentium 4.
- ✓ Memory: at least 256MB but we strongly suggest to at least have 512MB.
- ✓ If your operating system is Windows XP service pack 2 with built-in Firewall enabled, you must follow the steps below to open the ports: UDP/514, TCP/1080, and TCP/3306. In this way, all packets from or to the management server will not be blocked.

5. Go to Start > Settings > Network Connection.
6. Right click the Local Area Network and select Content.
7. Go to Advance > Settings > Exception and click the Connection Ports...
8. Enter the name and the port number to allow the following network ports.

Name	Port Number	Protocol
Log Server	514	UDP
Socks	1080	TCP
Database Server	3306	TCP
HTTP Server	80	TCP

FIGURE 3-1 Firewall settings of management server

3.2.2 Procedures

6. Install the Management Server
7. Install the AD Log Server
8. Upgraing the Management Server
9. Browsing the CD
10. Uninstall Management Server
11. Uninstall AD Log Server
12. Exit the Installation.

Figure 3-2 Management server software installation user interface

Note:

1. When you reinstall or upgrade your management server, please remember to reboot your computer. Only after you reboot the system can the system work properly. Detailed installation guide are shown in the QIG or User Manual.
2. If you have already installed any version of MySQL or Apache, you must uninstall MySQL and Apache before you start to install the management server. Please check Appendix for more details..

3.2.3 Installing Java Runtime

After you have installed the management server and plug in the wire, you can use web browser to connect to the management server by inputting http://<management server IP address>/ . When you first connect to the device, the software will check if your browser is able to run Java programs. If not, a Java Plug-in will pop up to remind you to install the Java runtime virtual machine onto your client system.

Note: When you first time connect to the management server, due to the size of the java runtime, the client must wait to download and install the Java Plug-In program. Please be patient.

3.3 Configuring Product

Before you start to manage the product, please use the RS-232 console to connect your PC to the device. You can also use SSH / Telnet or other terminal program to change the system parameters.

3.3.1 Starting the System

Turn on the power of the device, after the booting process, the system will prompt you with the user name and password. The default settings of the user name and password are admin & admin. After you have entered the system, you can use CLI command to change the password. Detailed CLI commands are listed in Appendix.

3.3.2 System Architecture

The product is transparently installed at the network exist without changing any existing network architecture. The management server together with the management system and reporting system will provide you a very easy-to-use interface for policy management. Administrators can setup a series of policy rules according to existing network architectures or companies policy. A single management server can control multiple devices, and can accept events/ logs from multiple devices. As long as you understand the basic installation steps, you can follow your network architecture to install the product. Detailed installation example is listed in the below figure.

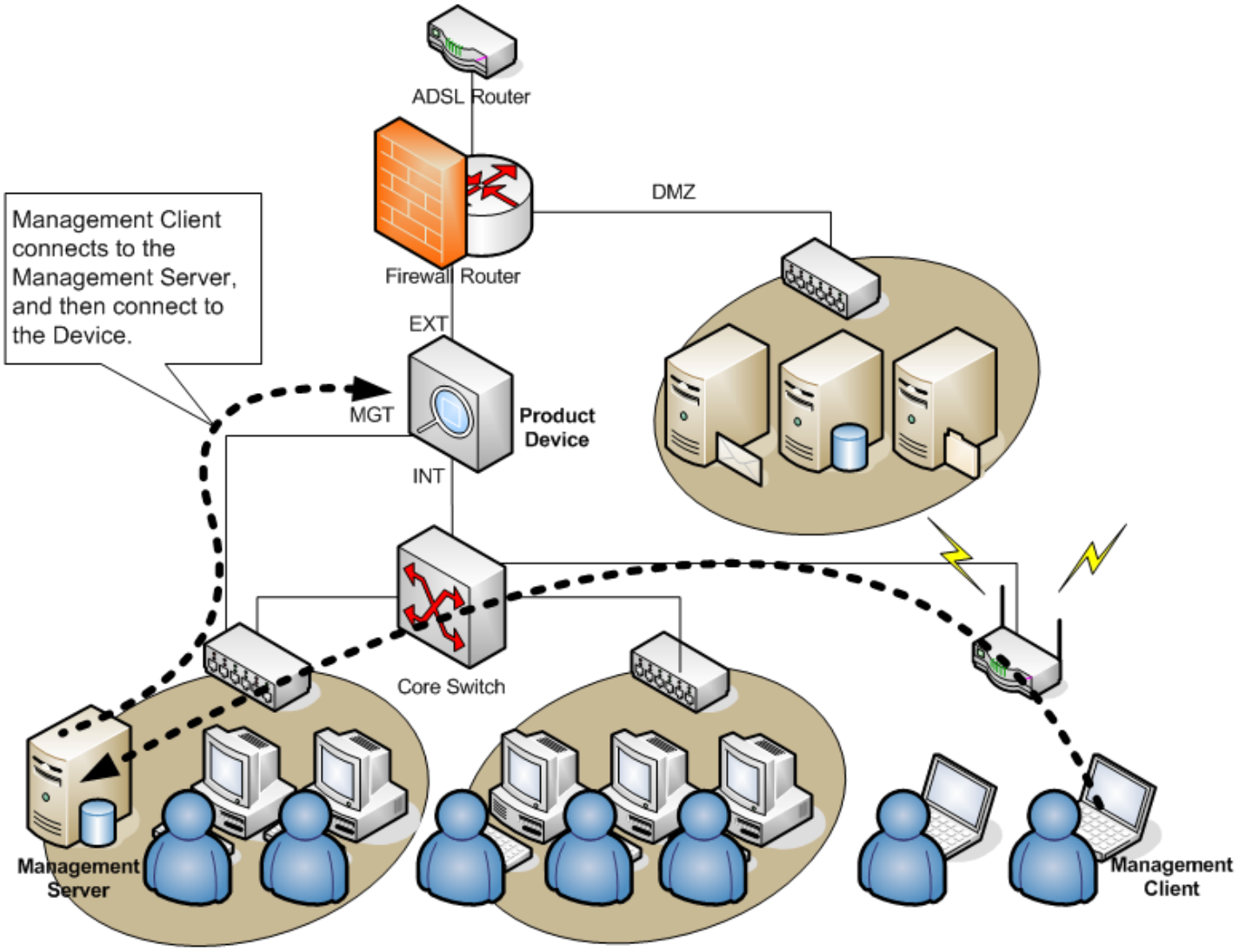


Figure 3-3 3-tier architecture example scenario

3.3.3 System Parameters

Use the RS-232 console cable to connect the device to the desktop PC. Please refer to the following HyperTerminal settings to setup the HyperTerminal.

Terminal Type	Hyper Terminal
bitrate	115200
date bit	8
synchonization	N
stop bit	1
Hardware flow control	N

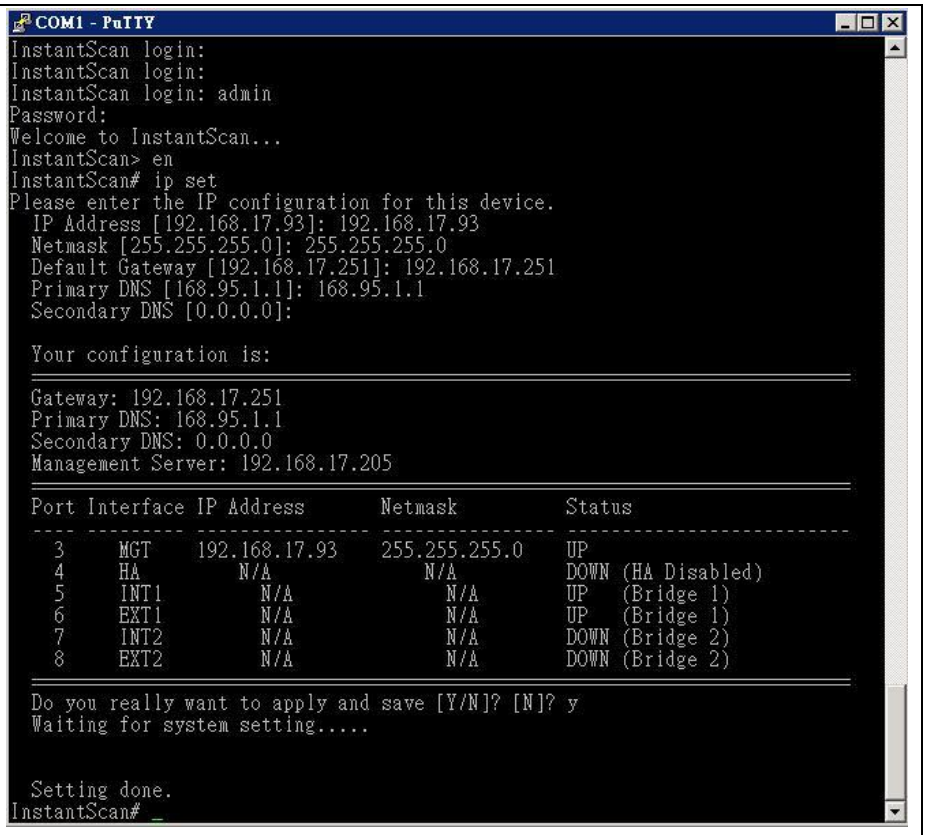
FIGURE 3-2 HyperTerminal settings

Step 1. Login system

The default ID and Password is **admin/admin**. After logging, you can use CLI commands to change the password.

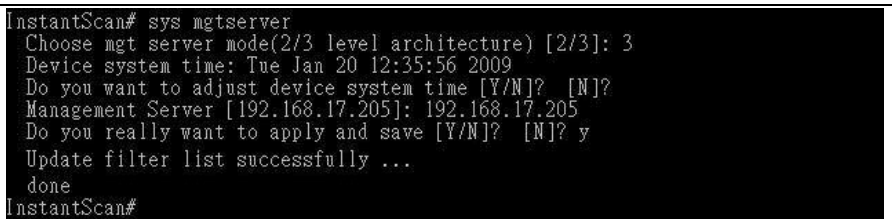
Step 2. Configure management port IP

Type "en**" to enter Privilege Mode. Type "**ip set**" command to configure the MGT interface and the Management Server related IP information.**



Step 3. Assign management server IP

Type "sys mgtserver**" to start assigning the device's management server.**



3.3.4 Connecting to Device

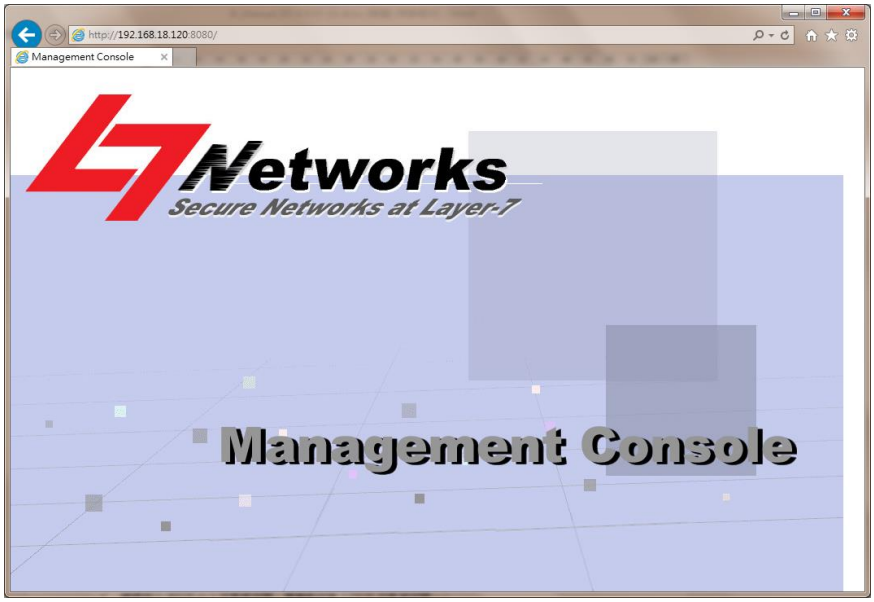
The product's management system uses Java applet technology. So you need to install Java virtual machine in your browser. **When you first connect to the management server with IE, you will be prompt to install the Java plug-in into your PC. After that, when you first login to the system, it requires a relatively long waiting time to download and run the program. Please be patient.**

Step 1 **Connecting to Mgt. Server**

Select an IP address for the management server to control the product (ex: 192.168.168.1). Open your IE browser and enter http://<management server IP>. For example, enter http://10.1.1.10 to connect to the management server. When the security alert window pops up, click OK to trust our java applet. Only when you click OK can the program successfully run on your system.

Note: If make your management server locate in the same subnet of your device.

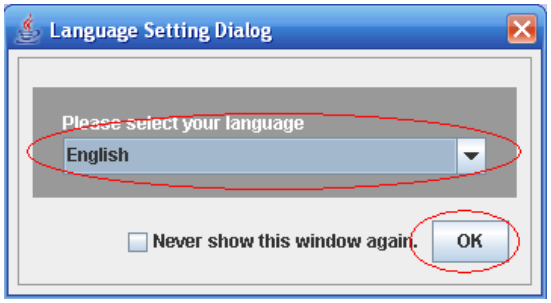
Connect to http://10.1.1.10



Step 2 **Choose the language**

The product currently offers several languages. You can select your favorite one to control the interface.

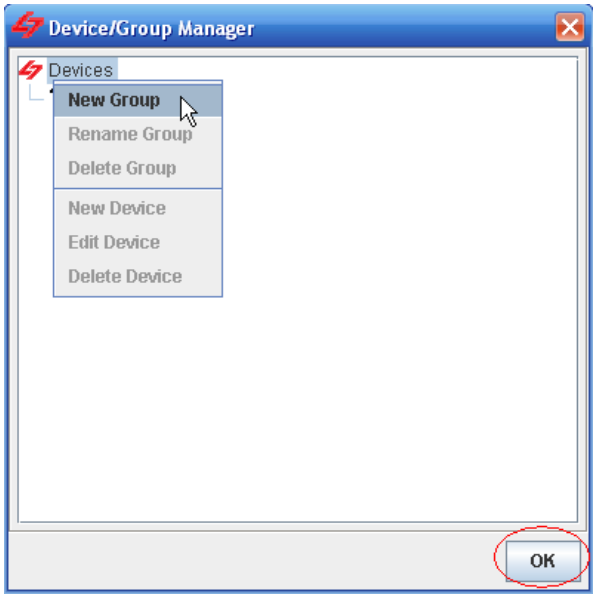
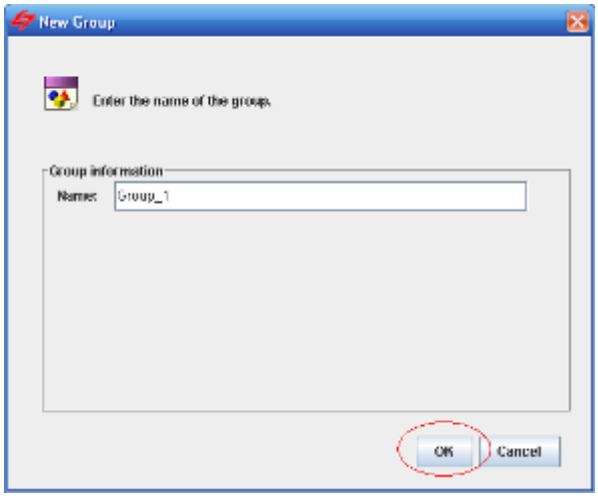
Note: After you have entered the login page, you have to go to **Tools > Language Setting** to change the language settings.



Step 3 **Login**

Enter the username and password (default admin / admin). After that, you will enter the system.

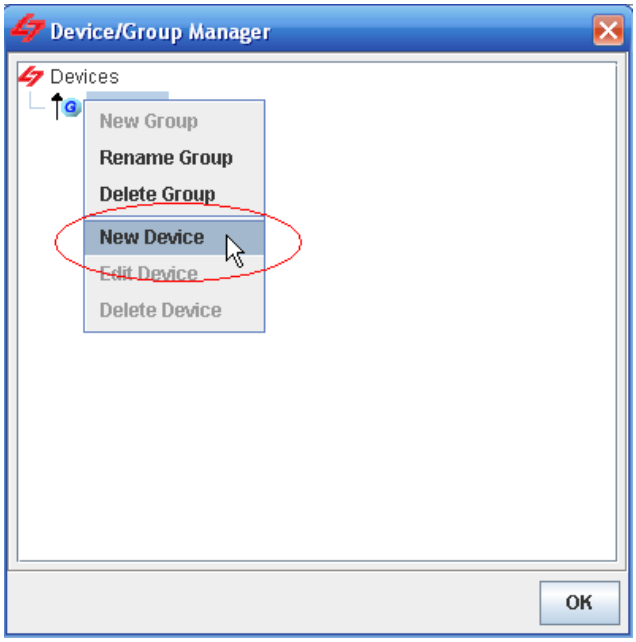
3.3.4.1 Creating Devices/Groups

Step 1 **Adding device / group** After you successfully enter the system, please click the item **Device/Group Manager** to add a new device or group.	**File > Device/Group Manager** 
Step 2 **Adding a group** Right click at the Devices item, and select the **New Group**.	**File > Device/Group Manager > New Group** 
Step 3 **Input the Group name** Input the name of the group and then click the OK button to continue. After that, the group name will display on the screen. You can right click the item and select **Rename Group** or **Delete Group** to modify or delete the group.	**File > Device/Group Manager > New Group** 

Step 4 **Creating New Device**

Right click on the existing group **Group_1** and select **New Device** to add a new device.

File > Device/Group Manager > New Device

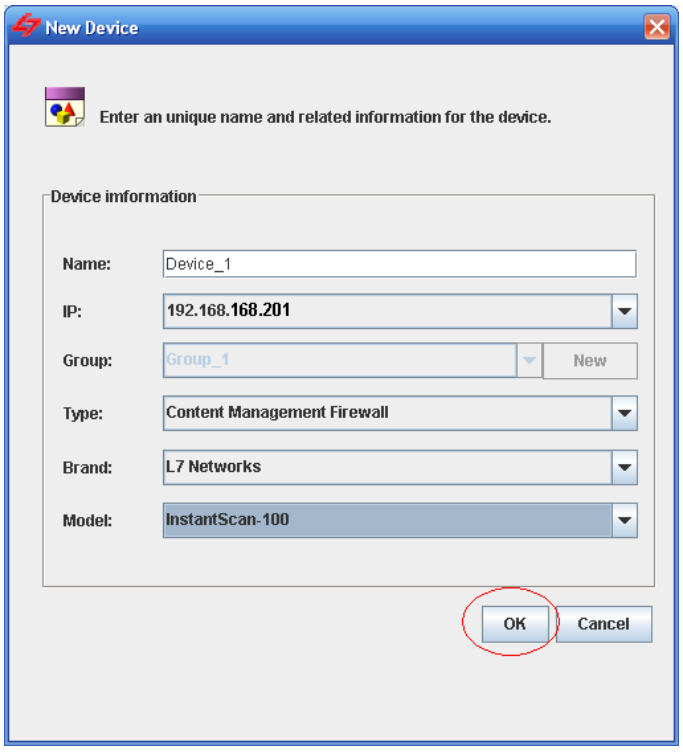


Step 5 **Edit related device information**

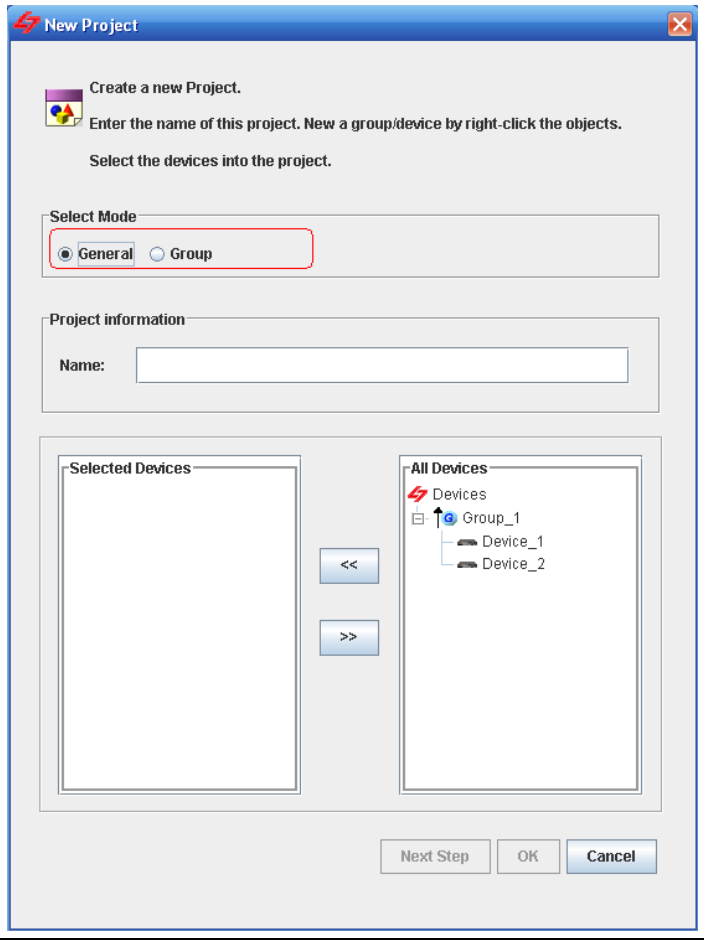
Input the device name and select an IP address which is previously registered by the ip set command of the device. Click the **OK** button to store the settings.

Note: You must setup the IP address from the device first before you can add a new device. After you have added a device with the right Figure, the IP address will not appear again when you add another new device.

File > Device/Group Manager > New Device



3.3.4.2 Creating a Project

Step 1 **Creating a new project** Select **New Project** to create a new project.	**File > New Project** 
Step 2 **Creating a new project** First, please check the Project Mode, Project Name, and select the wanted devices from the **All Devices** tree-like field. Then click the **<<** button to add your chosen devices to the **Selected Devices** field. If you want to remove some devices from the current project, click the **>>** button to remove your selected devices.	**File > New Project > New Project** 

Project Mode	Description
General	If you want each of your devices has individual settings, choose this mode.
Group	If you want each of your devices has the same settings, choose this mode. Moreover, when you use this mode, all data will be integrated into the same report system. No matter which device you have modified, the settings will be updated to the Base Device configuration. Other devices will refer to the Base Device as its configuration.

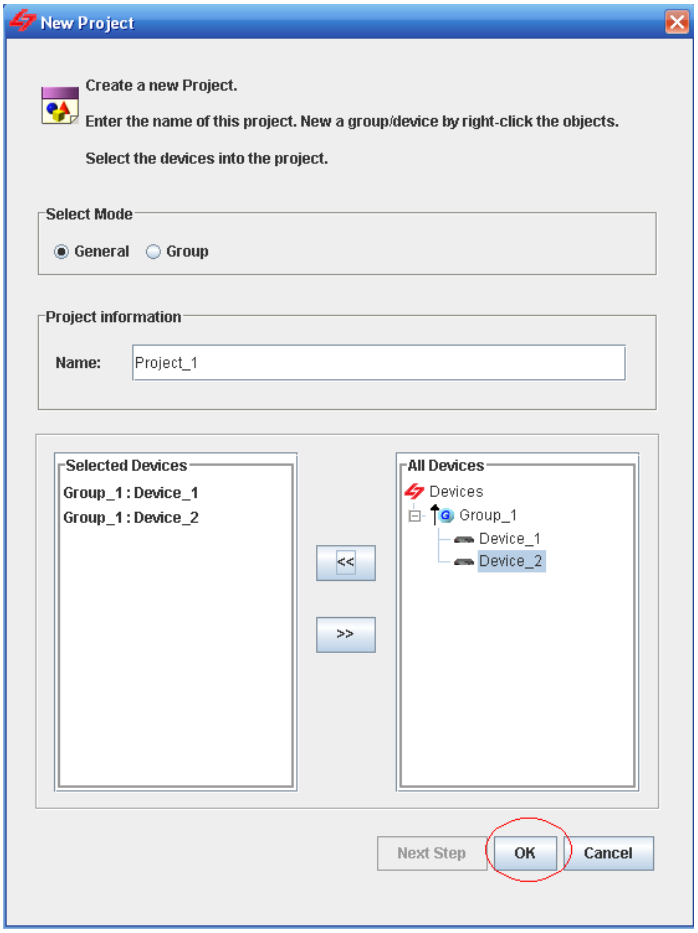
FIGURE 3-3 Project mode

General Mode

Step 1 Creating a new project

Select **General** as the project mode. This mode is suiFigure for most cases. Enter the project name and select devices from the right column. Click the **<<** to move the device from right to left.If you want to remove some devices from the current project, select the device in the left column and click the >> button. Click the **OK** button to finish the settings.

File > New Project

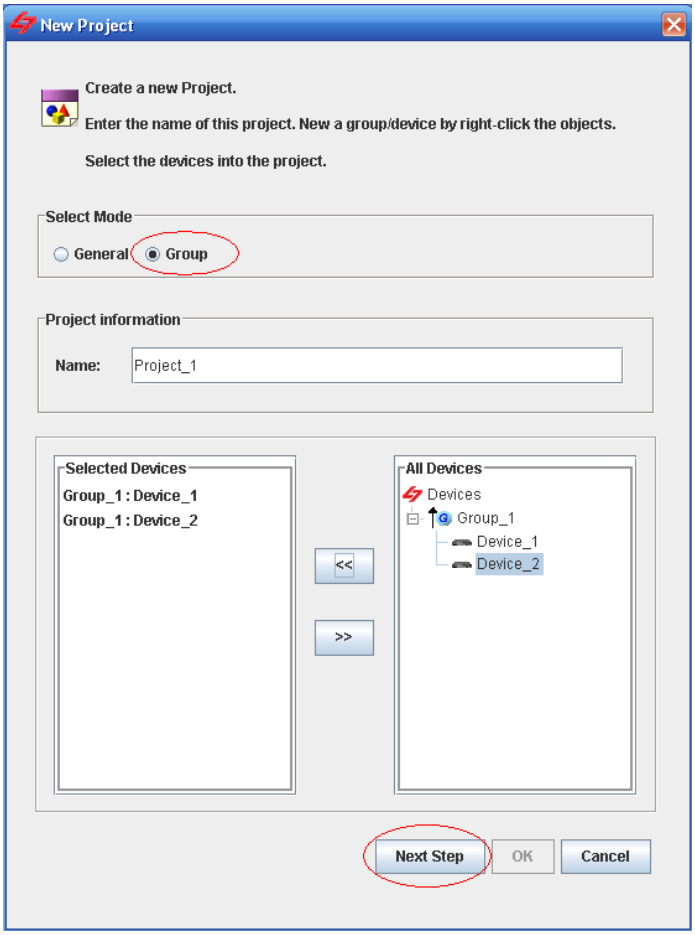


Group Mode

Step 1 Creat a group-mode project

Select **Group** as the project mode. This mode is suiFigure for someone who buys several device and puts them in different network edges. Enter the project name and select devices from the right column. Click the **<<** to move the device from right to left.If you want to remove some devices from the current project, select the device in the left column and click the >> button. Click the **OK** button to finish the settings.

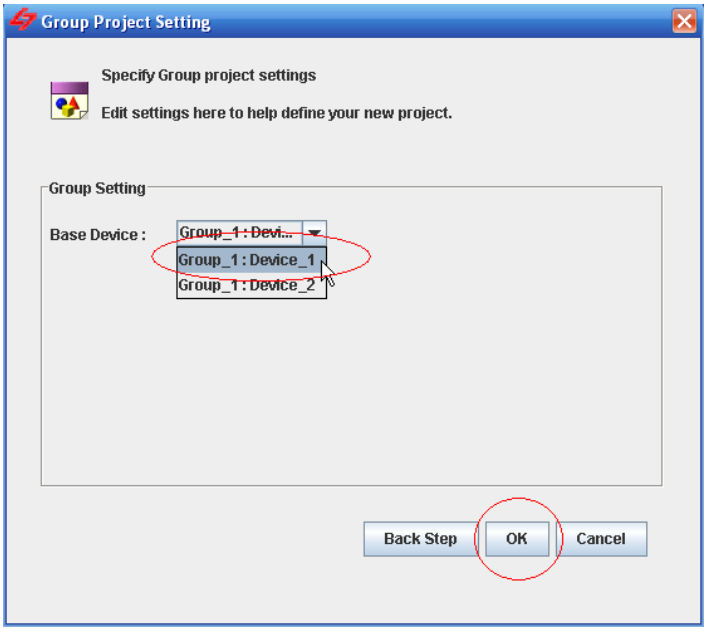
File > New Project



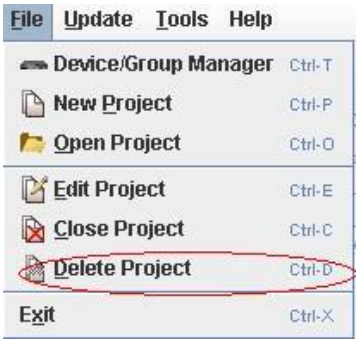
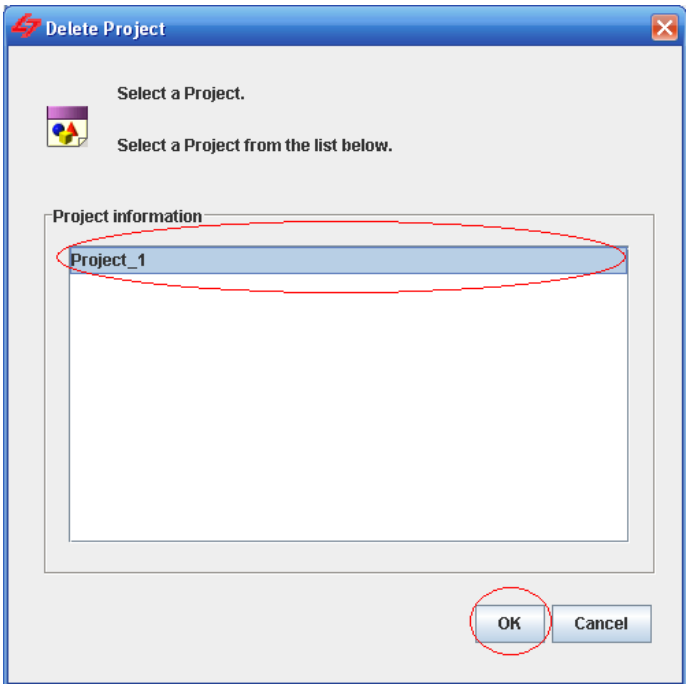
Step 2 Choose the base device

Select a device as your **Base Device**. When you select the base device, all other devices in this group will refer to the configuration of the base device. Moreover, the report of all statistics is aggregated from all the devices in this project. Click the **OK** button to finish the settings.

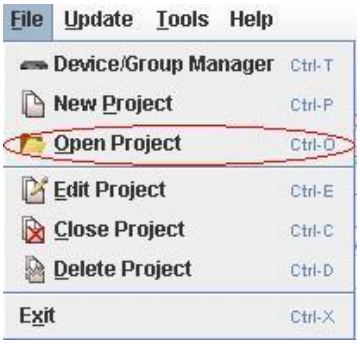
File > New Project > Next Step

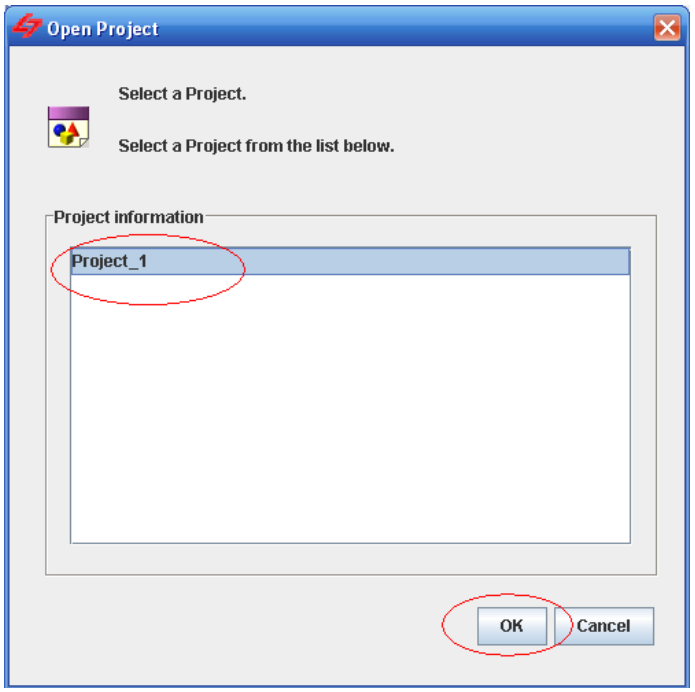
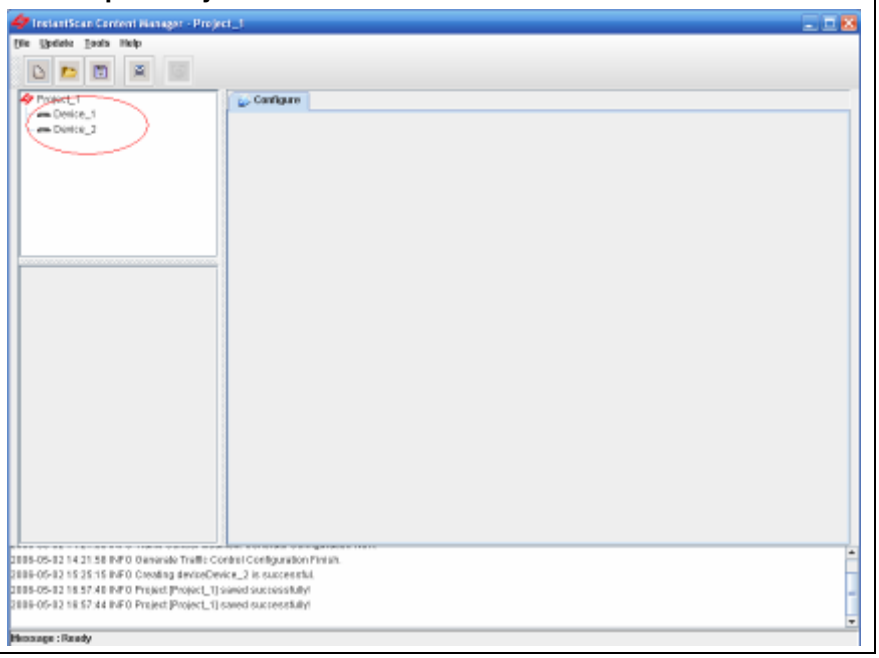


3.3.4.3 Deleting a Project

Step 1 Click the Delete Project Check the **Delete Project** option.	**File > Delete Project** 
Step 2 Deleting a project Select the project you want to delete and click the **OK** button to continue. **Note:** 1. Once you click the OK button, the project will be immediately removed from the system. 2. Running project cannot be removed. You must close the project first and then remove the project.	**File > Delete Project** 

3.3.4.4 Open an Existing Project

Step 1 Open project Click the **Open Project** item.	**File > Open Project** 

Step 2 Select a project to open Select a project you want to open and clickthe the **OK** button to continue.	**File > Open Project** 
Step 3 Start managing the product Now you can start managing your product. A single project can control multiple device belonging to different groups. Move the cursor to the device you want to manage and double click it, the system will connect to the device and load the configuration to the management console screen.	**File > Open Project** 

Part 2

Design Philosophy

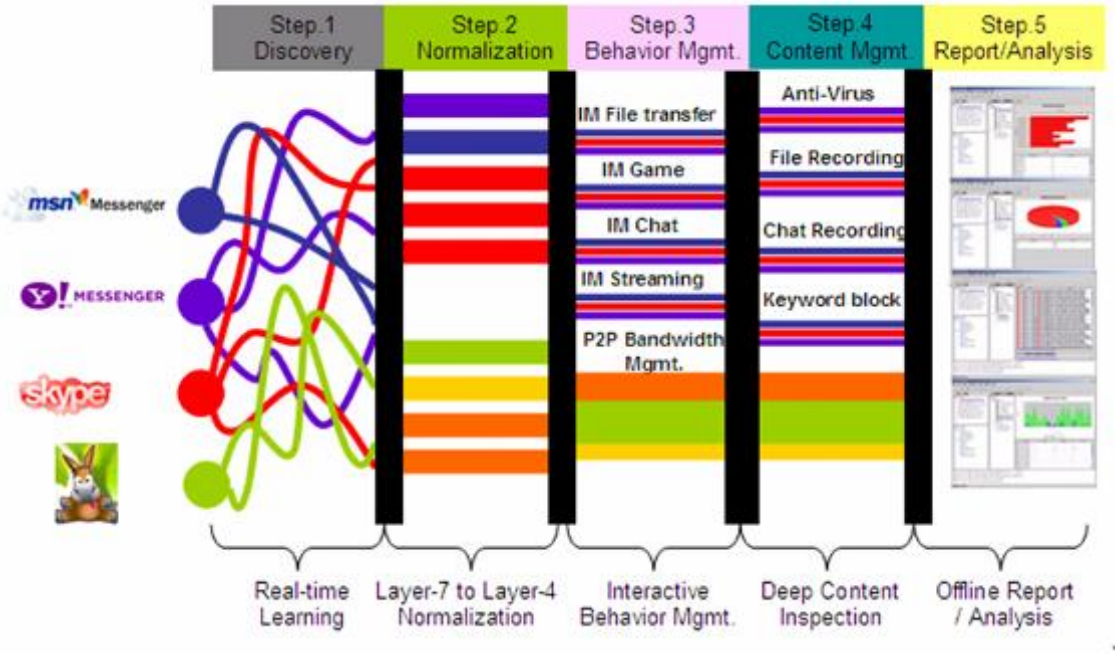
Chapter 4
Internal Data Processing Flow

This chapter introduces the basic design principle and the steps to achieve the principle

4.1 Technology

Nowadays, many Internet users have installed IM and P2P applications which apply port-hopping and HTTP-tunnelling to avoid being checked or blocked. To help MIS to overcome the issues, 5-step Content Management is proposed to maximize the productivity / security and minimize the threats / TCO (Total Cost of Ownership).

5-Step Content Management: Maximize Productivity/Security, Minimize Theats/TCO



1. **Step 1. Plug & Play Real-time Discovery/Learning**: To help the network administrators solve the above problems, Product provides the Plug & Play Discovery as the step-1 procedure. Just plug in the wire and the Product will replay the network traffic in real time. You can see how many MSN tunnelled in the HTTP, and see how many IM peers are chatting. The chatting process will automatically be learned by Product and can be further imported to your configuration.
2. **Step 2. Layer-7 to Layer-4 Normalization**: After discovering for a while, if you decide to manage the traffic, you can start to block something using the App Policy. In the Figure, the Product has normalize the traffic. The MIS can easily control the Product just like what layer-4 firewalls can do. Furthermore, the Product can help you stop non-standard IM connection. For example, the MSN will automatically detect the firewall settings. If the MSN cannot find a way out through standard port 1863, it will try to connect to an HTTP proxy. However, anyone can manually conFigure his/her MSN settings to use any HTTP/SOCKS4/SOCKS5 proxies in the world, including those in your company. What is worse, users can connect to many WebIM pages to chat with their browsers. The Product can help you handle those situations.
3. **Step 3. Interactive Behavior Management**: Nevertheless, the MIS would like to do individual policy settings. Since the Product can recognized the detailed behaviors of each application, the MIS can setup individual policies. The user's information can be easily integrated with enterprises' user database, such as LDAP, Active Directory, POP3(S), IMAP(S), and RADIUS.

4. **Step 4. Deep Content Inspection**: The MIS may also want to do advanced filtering of the contents. In the Figure, the Product can detect/block viruses in compressed files and worms spread in IM windows. For extreme security, the conversations can be recorded. And if the users violate the policy to say forbidden keywords, the Product will instantly inform the users the company's IM policy.
5. **Step 5. Offline Report/Analysis**: Finally, reporting and analysis can help the MIS to find out the problem. Tens of graphical reports are presented, including daily/weekly/monthly bandwidth usage, IM behavior, conversation recording, and policy violation. Reports can be customized, searched, and emailed with PDF/HTML attachment by user-defined schedule.

4.2 Procedures

The product can control the most popular Instant Messengers (IM), Peer-to-Peer (P2P), Remote control, VoIP applications, and Web contents. You can make use of these tool to manage your network to prevent information leakage or wake up the productivity of some employees. It can not only block those applications but can manage them by behavior or contents. In the following sections, we will focus on how to overcome the problems in your networks.

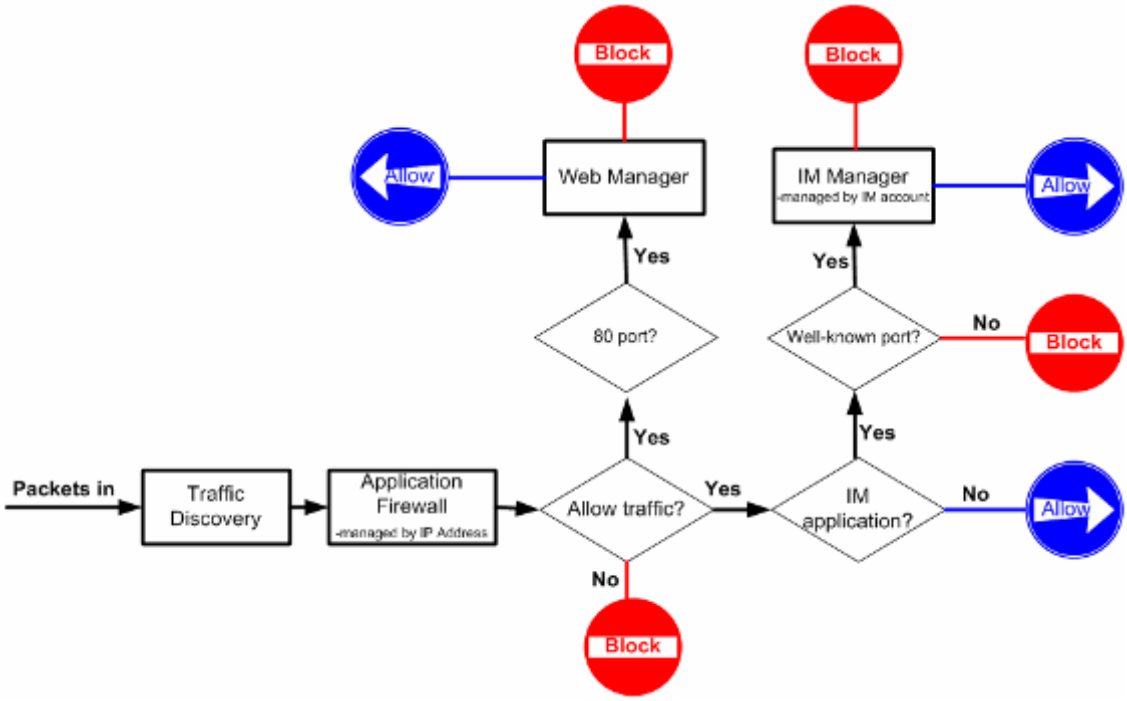


FIGURE 4-1 Traffic flow in the device

As displayed in FIGURE 4-1, the traffic flow through the device will be first enter the Traffic Discovery module (Monitor->Realtime) to do layer-7 deep packet inspection, followed by the App Policy module to block unwanted applications. No matter the application use HTTP/SOCKS tunnels to cheat IT experts, all packets are analyzed by the layer-7 packet inspection engine. Subsequently, the App Policy will judge the final result by the source / destination IP addresses and the real application name (instead of port number).

When you enable the Web Manager, all web traffic will be analyzed to see if the content of the traffic should be blocked or not. A built-in URL database can quickly check for unwanted websites and return warning message to the user immediately. Moreover, the URL access history of each person can be fully recorded for further investigation.

If you enable the IM Manager, the traffic will be anaylized to see if the IM traffic contains illegal contents or activities. All famous IM, such as MSN / Yahoo / AIM / ICQ will automatically cheat the firewall with port-hopping behavior. The IM Manager will stop their port-hopping traffic and only allow them to use their standard ports. Their standard ports are 1863, 5050, 5190, and 5190 correspondingly. So once you enable the IM Manager, for example, MSN over HTTP will be blocked

by the IM Manager. As a result, the MSN will be force to go in its standard port: 1863. The device then just needs to check for standard ports. This is a balance between performance and convenience. If your Firewall does not open outbound port 1863, you need to open that to let the MSN traffic pass through its standard way. If you really don't want to open any other outbound ports except for port 80, you need to start the Encapsulation Manager, which allows you to manage the IM / Web contents even the IM / Web traffic goes in HTTP / SOCKS tunnels through proxies.

4.3 User Interface

The system contains 5 windows area:

1. **Toolbar:** This area includes menu items and quick configuration buttons.
2. **Project:** This area lists the devices in the opened project.
3. **Function:** After you double click one device, this area will show you the available functions of the device. The functions are categorized into Monitor, Management, and Report groups.
4. **Management:** After you single click on any one of the item in the function list, this area will show the details of the function.
5. **Status:** Any messages will be put into this area for you to know the status of the configuration. You can push the  icon to hide the status area.

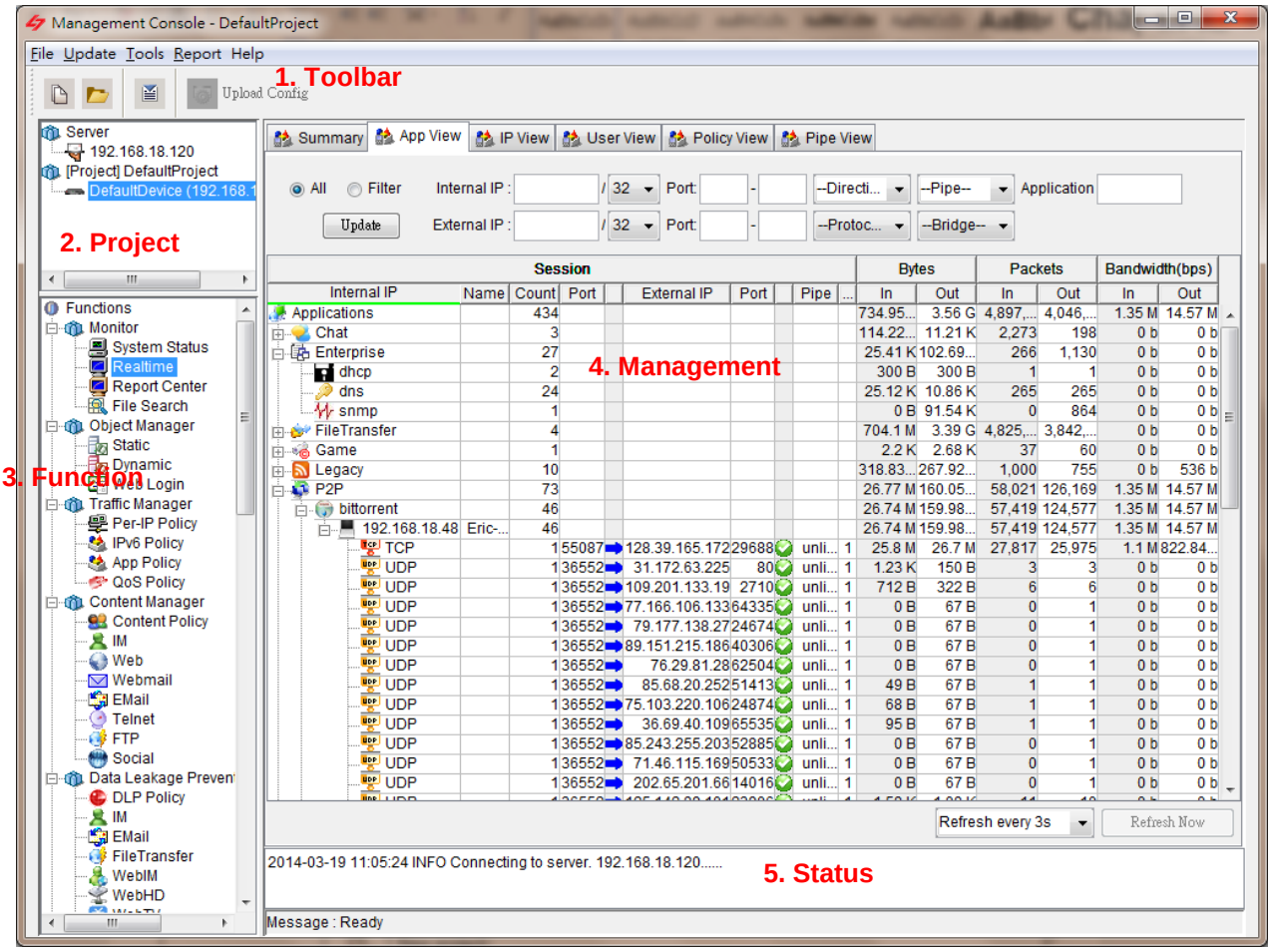


FIGURE4-2 Layout of the user interface

4.4 Icons

Icon		Function
Toolbar		New project
		Open project

		Display / Hide the status area
		Upload config
Management		Group object
		Host object
		Inverse of the selected group object
		Inverse of the selected host object
		Date options for you to select the date
		Advanced search function that can customize the search criteria
		Setup the refresh period
		Settings for report export

FIGURE 4-1 Description of all icons

4.5 Toolbar

Item	Sub item	Description
File	Device/Group Manager	Create new devices or groups
	New Project	Create a new project
	Open Project	Open a new project
	Close Project	Close the current project
	Delete Project	Delete the selected project
	Exit	Quick the graphical user interface
Update	Upload Configuration	Upload config to the device
	Register	Register the product. *Before updating the application patterns and url / virus database, you must register first.
	Update IM engine	Update the IM engine from the update center
	Update pattern	Update the application patterns from the update center
	Update AV database	Update the anti-virus database from the update center
	Update URL database	Update the URL database from the update center
	License	Enter the trial or deal license here. By default several functions are in trial mode and will disfunction after 5 days. After that, the device goes into bypass mode to only forward the traffic. You must reboot it make it function in another 5 days. You can request a longer trial license from your reseller. Input the license here to make it effective. Once you have purchase the product, your reseller will offer you a permanent deal license that will make the device function permanently without reboot. Note that you must register first before you can enter any license here.
	Option	Settings for the update center
	Support list	The application patterns that is supported in the current device.
Tools	Account Manager	Setup for the permission of each login account to the system
	Change Password	Change the password of the current login user
	Language Setting	Select the language of your preference
	SNMP Control	Settings for the SNMP protocol
	Config Backup	Backup the current config to the local disk
	Config Restore	Restore the config in the local disk to the device
Help	About	Display the version information

4.6 Versions

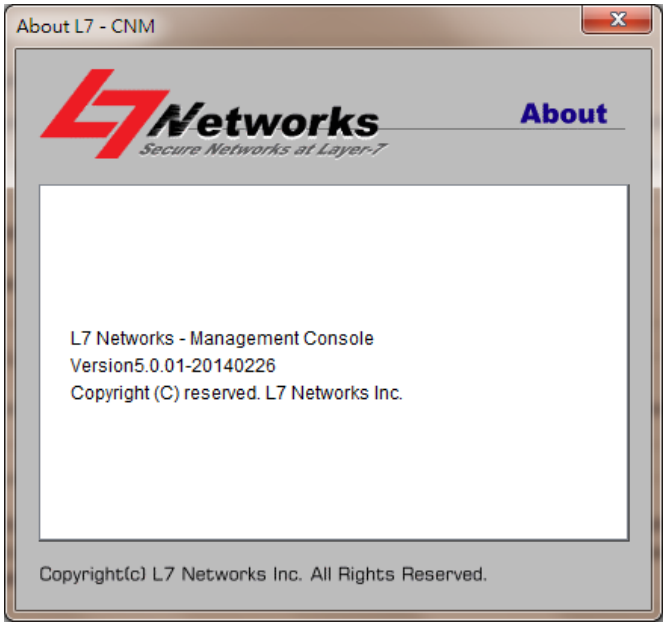
Step 1 **Lookup the version of mgt server** The firmware of the product must match the version of the management server. Please click the **About** to check for version.	**Help > About** 

Step 2 **Version display**

After the About is invoked, the Figure will show you the version in details.

Note: The version consistency between the device and the management server lies in the first two segment of a version number. For example, in this example, the management server is in version 2.2.01. This software will apply to all 2.2-based devices. Namely, devices ranging from version 2.2.0 to 2.2.13 can use this management software. Only 2.2 matters. The following numbers do not count.

Help > About



Part 3

Network Monitoring

Chapter 5
Traffic Discovery

This chapter shows you how to catch internal thieves to further setup policy rules to manage them

5.1 What Is On Your Networks?

The often-heard advice to "know your network" is needed by broadband and WAN operators more than ever before. Being able to identify the applications and users on the network, and to quantify and analyze the traffic they generate is an essential first step to capacity planning, to subscriber demographics and service optimization. Without granular visibility into network traffic, you are simply working blind.

Step 1 Monitor the network

Double click the Protocol in the Traffic Discovery area, you can easily track the network connections passing through the device. Connections marked in red are non-standard connections which we called the tunnelled traffic. That kind of traffic will be blocked once you enable the IM Manager.

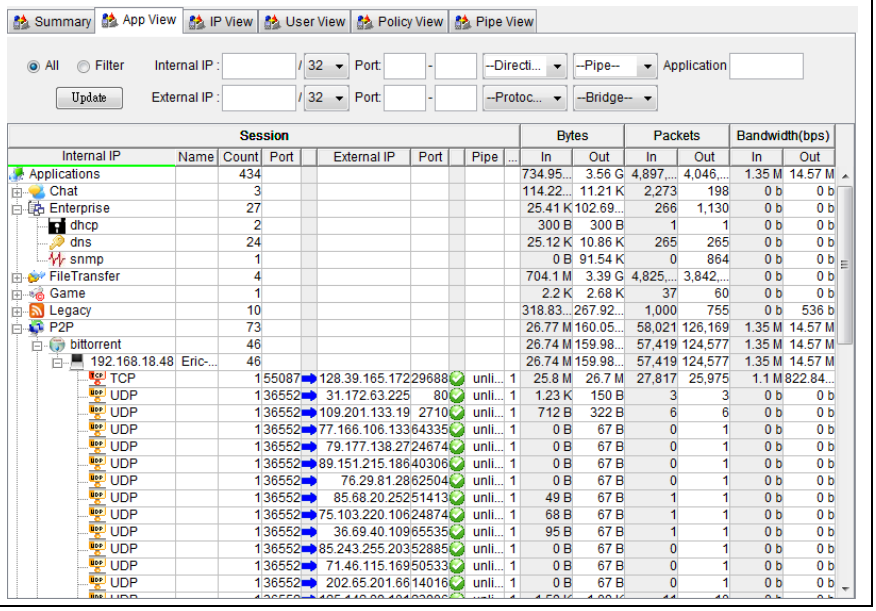
Note: The stand ports for IM are:

MSN：1863

Yahoo：5050

AIM/ICQ：5190

Function > Monitor > Realtime

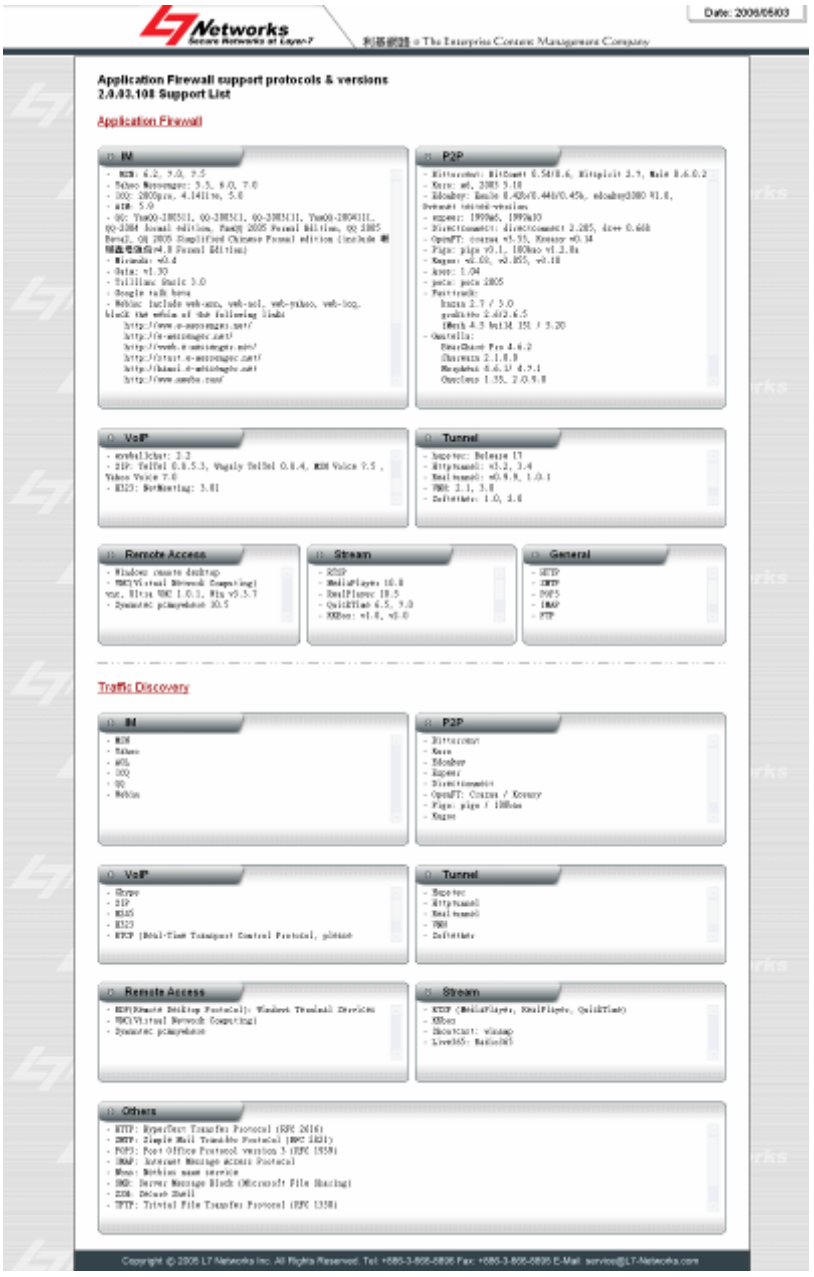


Field	Description	Example
Type	The protocol hierarchy of the pass through connections	msn
Src IP	Source IP address of the connection	192.168.17.58
Src port	Source port of the connection	3684
Dest IP	Destination IP address of the connection	192.168.17.190
Dest port	Destination port of the connection	3128
In byte	Inbound number of bytes transferred	12929
out byte	Outbound number of bytes transferred	3028

FIGURE 5-1Realtime traffic discovery fields

Step 2 Display supported applications

You can go to our official website and click the release note of each pattern release. There will be a support list hyperlink to describe the protocol/application that is supported in that version of pattern.



Part 4

Traffoc Manager

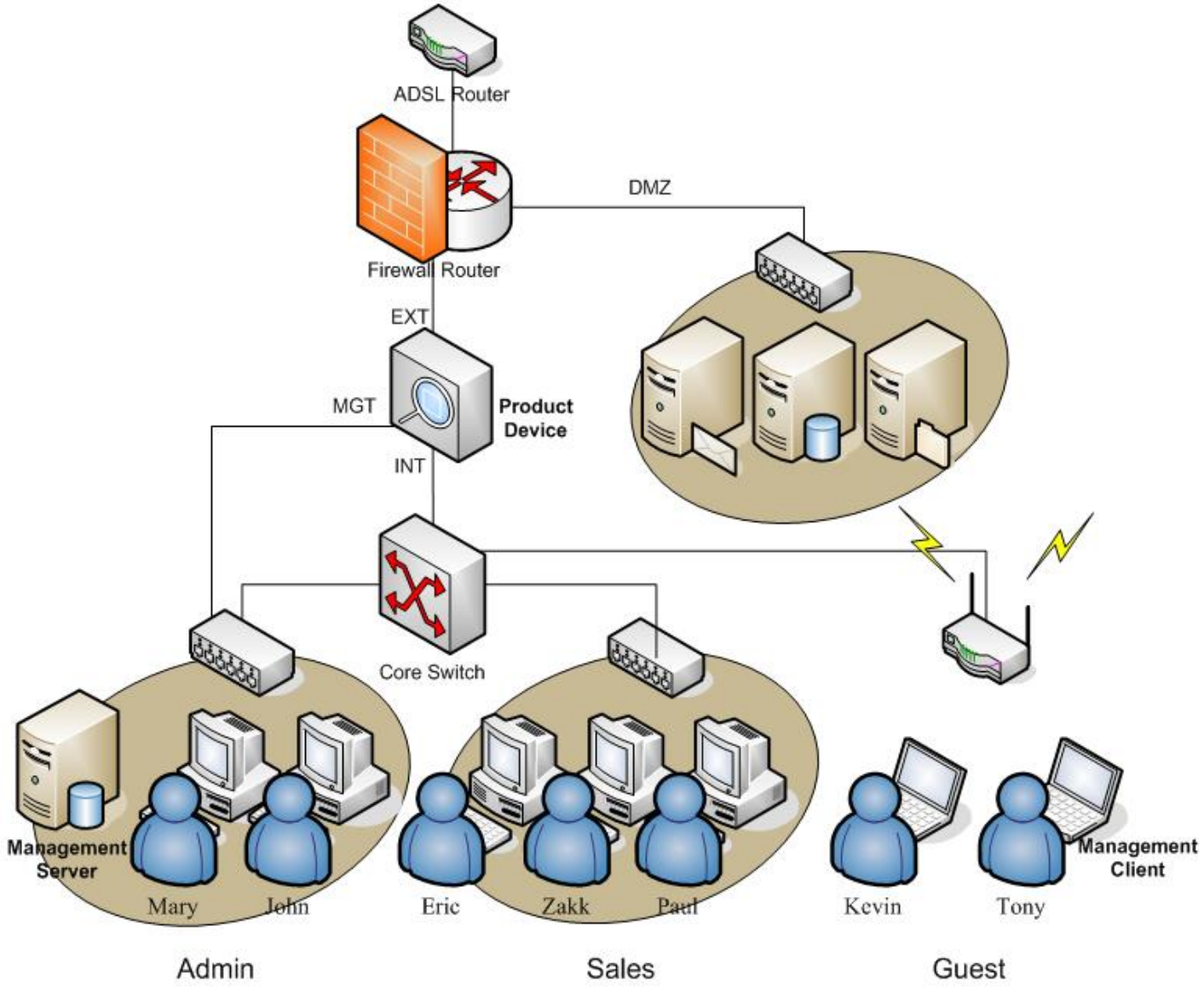
Chapter 6
Per-IP Manager

This chapter introduces how the Per-IP Manager works for your needs.

Per-IP Manager can setup many limits for each internal IP addresses, such as session count, upload rate, download rate, and hourly/daily/weekly quota.

6.1 Scenario

John and Marry belong to the group Admin. Paul, Zakk, and Eric belong to the group Sales. The members in group Admin are nearly unlimited in session count and bandwidth. The members in group Sales are limited to have 200 sessions and 1Mbps upload bandwidth and 1Mbps download bandwidth. What is more, each IP should have a limited P2P usage: only allowed to occupy 100 sessions of the total 200 sessions, o.5Mbps of the 1Mbps upload bandwidth, and 0.5 Mbps of the download bandwidth.



6.2 Methodology

The product should first setup a default policy for all IP address to have an initial limit for the session count, upload bandwidth and the download bandwidth as follows. Then define the general limits for the members in the group Admin. Then define the general limits for the members in the group Sales. Finally you will have to define the sub rule for the group Sales. Add a per-ip app policy rule for the group sales as follows.

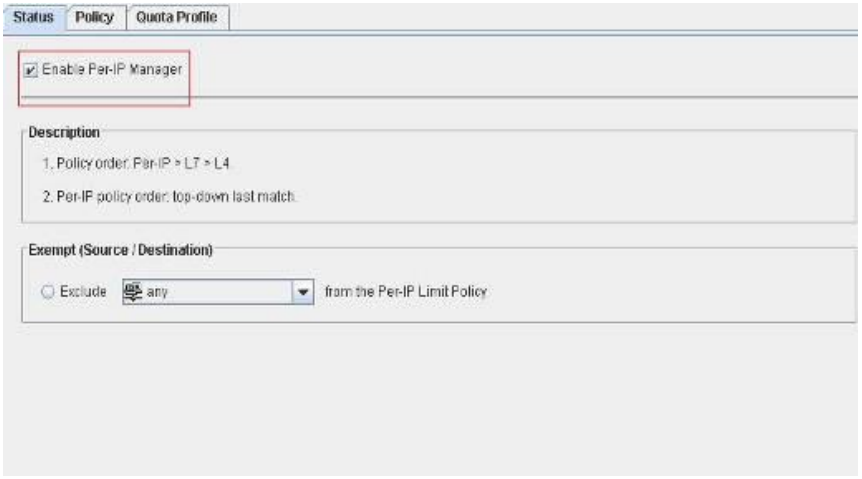
Internal Users	Service	Session count	Bandwidth	
any	Any	0	Upload	1000Mbps
			Download	1000Mbps
Admin	Any	0	Upload	1000Mbps
			Download	1000Mbps
Sales	Any	200	Upload	1 Mbps
			Download	1 Mbps
Sales	P2P	100	Upload	0.5 Mbp
			Download	0.5 Mbps

6.3 Steps

Step 1 **Start the Per-IP Manager**

Check the **Enable Per-IP Manager. If you want to add some IPs in the excluding list, click the Exclude radio box and select the interested group.**

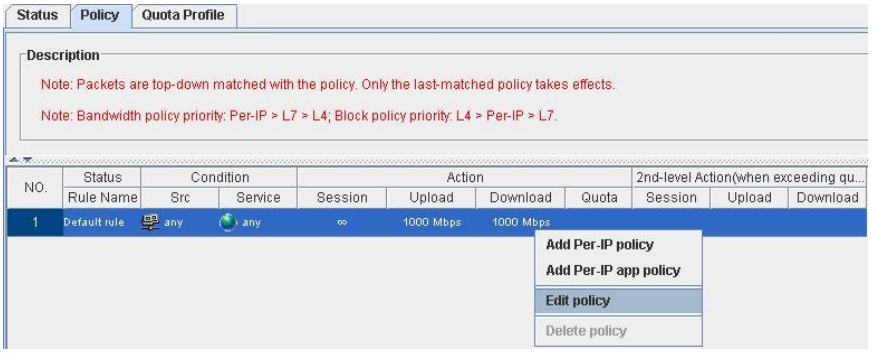
Management > Per-IP Limit Manager > Status



Step 2 **Edit the Default Rule**

Right click the Any ruleand select the **Edit Policy.**

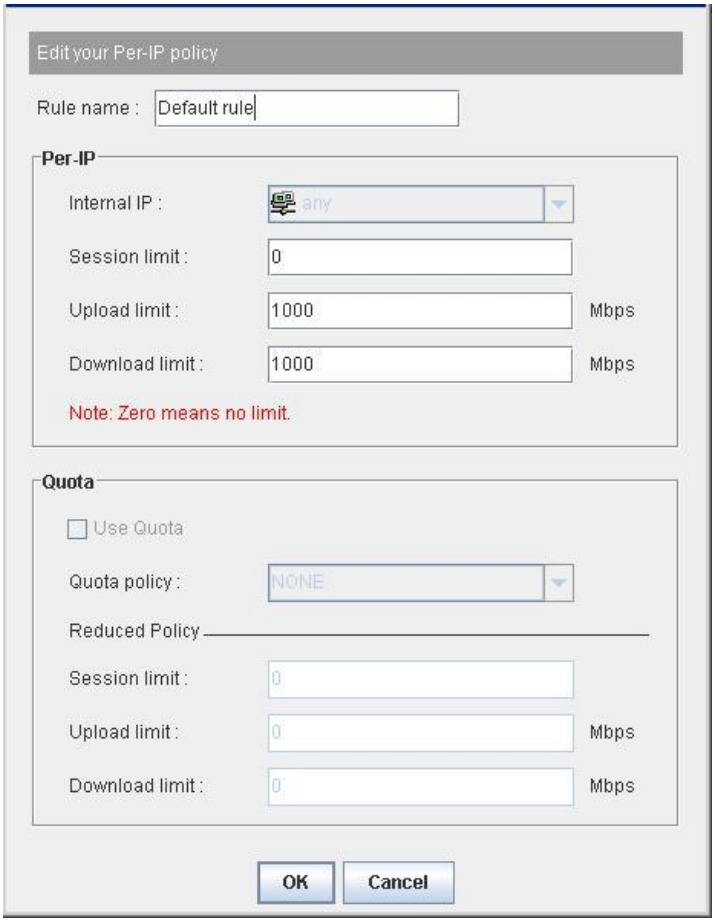
Management > Per-IP Limit Manager > Policy



Step 3 **Edit the Default Rule**

Right click the Any ruleand select the **Edit Policy.**

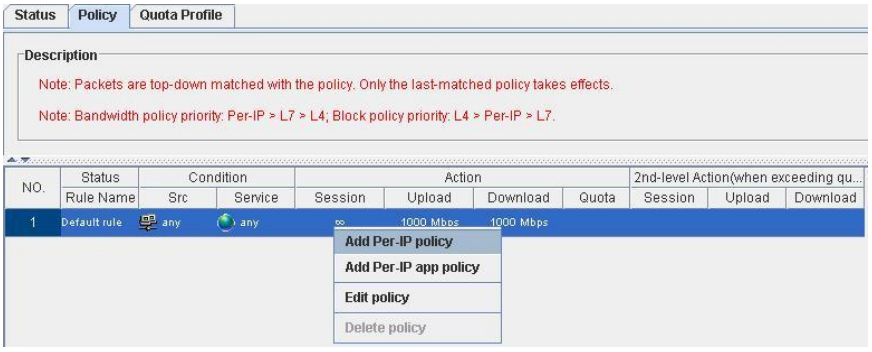
Management > Per-IP Limit Manager > Policy



Step 4 **Edit the Default Rule**

Right click the Any ruleand select the **Edit Policy.**

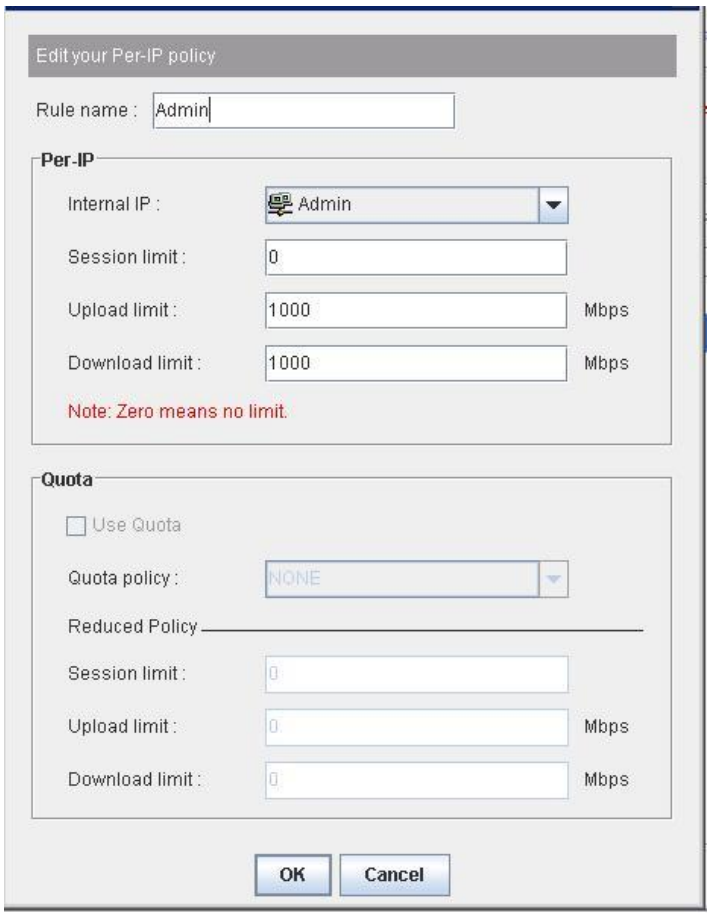
Management > Per-IP Limit Manager > Policy



Step 5 **Limit the session/ bandwidth**

Change the session limit to 0 (unlimited) and upload/download bandwidth to 1000 Mbps. Note that 0 means unlimited.

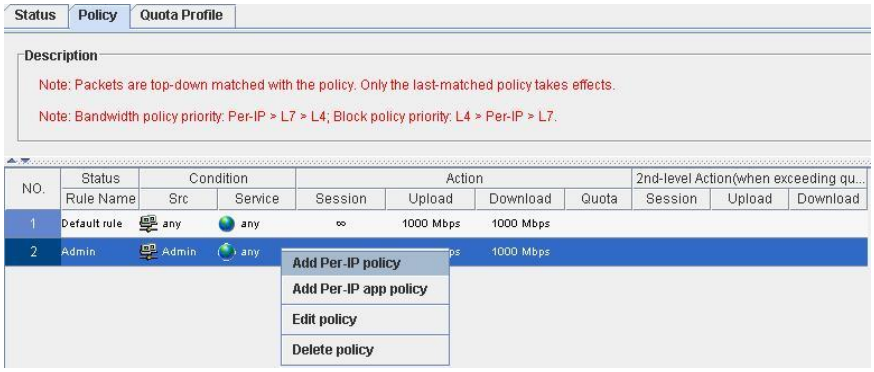
Management > Per-IP Limit Manager > Policy



Step 6 **Add a new rule**

Right click to add a new rule for “UnLimitedGroup”.

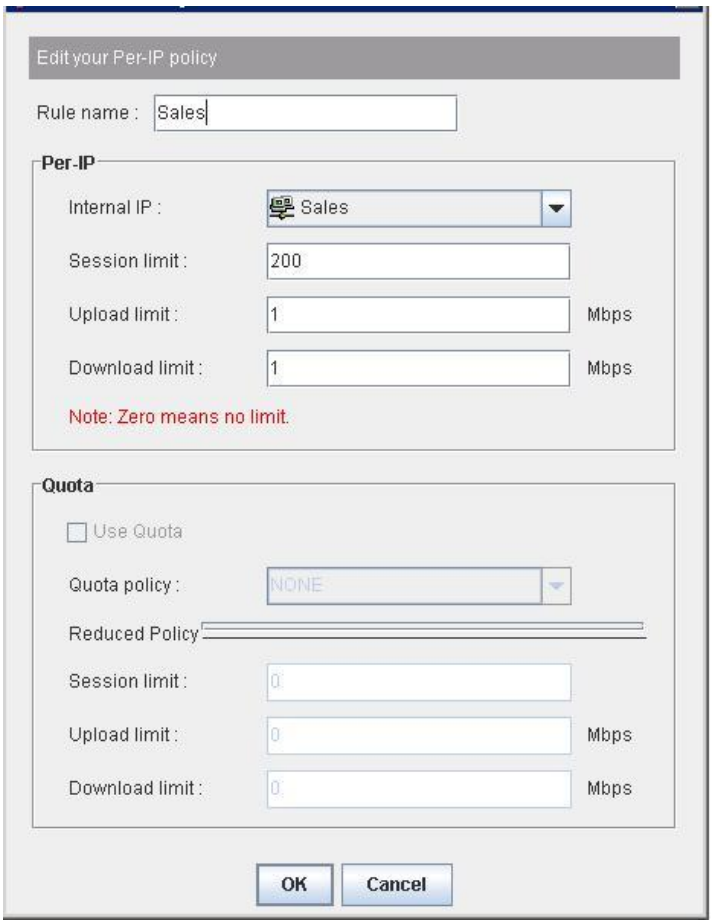
Functions > Traffic Manager > App Policy



Step 7 **Edit the new rule**

Select the UnlimitedGroup and enter 100 Mbps for the download limit, 100 Mbps for the upload limit. In this way, those IP in the UnlimitedGroup will have a max 100Mbps bidirectionally.

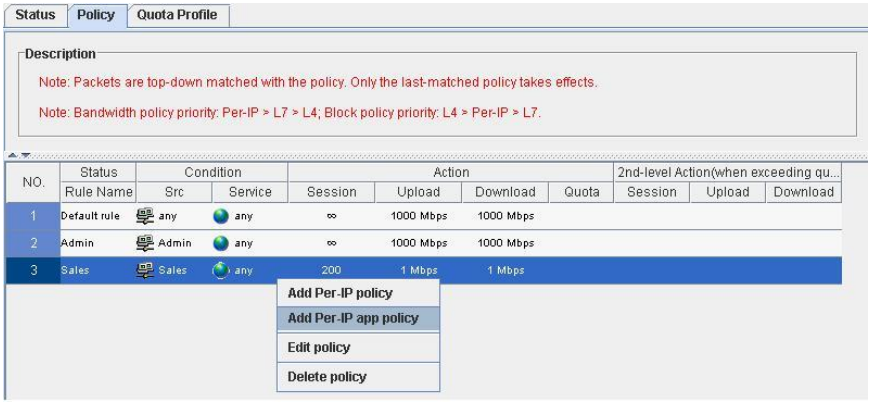
Management > Per-IP Limit Manager > Policy



Step 8 **Add a per-app rule**

Right click the UnlimitedGroup rule, and select the add per-app policy. You can setup extra limits for the applications. Select the UnlimitedGroup and enter 100 Mbps for the download limit, 100 Mbps for the upload limit. In this way, those IP in the UnlimitedGroup will have a max 100Mbps bidirectionally.

Management > Per-IP Limit Manager > Policy



Step 9 **Edit the new rule**

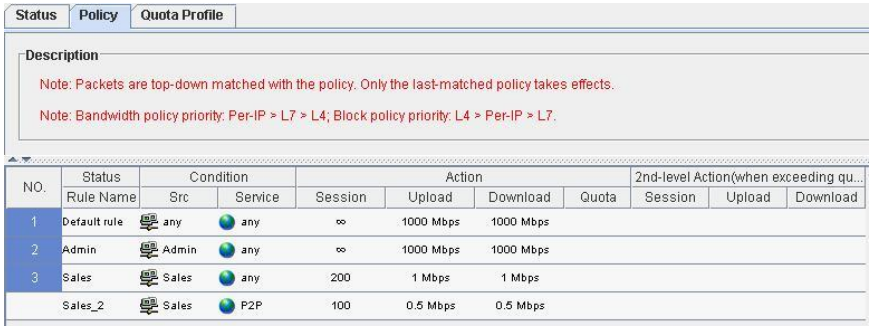
Select the UnlimitedGroup and enter 100 Mbps for the download limit, 100 Mbps for the upload limit. In this way, those IP in the UnlimitedGroup will have a max 100Mbps bidirectionally.

Management > Per-IP Limit Manager > Policy

Step 10 **Edit the new rule**

Select the UnlimitedGroup and enter 100 Mbps for the download limit, 100 Mbps for the upload limit. In this way, those IP in the UnlimitedGroup will have a max 100Mbps bidirectionally.

Management > Per-IP Limit Manager > Policy



NO.	Status	Condition		Action				2nd-level Action(when exceeding qu...		
	Rule Name	Src	Service	Session	Upload	Download	Quota	Session	Upload	Download
1	Default rule	any	any	∞	1000 Mbps	1000 Mbps				
2	Admin	Admin	any	∞	1000 Mbps	1000 Mbps				
3	Sales	Sales	any	200	1 Mbps	1 Mbps				
	Sales_2	Sales	P2P	100	0.5 Mbps	0.5 Mbps				

Chapter 7
Traffic Manager

This chapter introduces how the Traffic Manager works for your needs.

People often use Outlook to receive emails, Internet Explorer to browse websites, IM such as MSN/Skype to communicate with friends, and P2P such as KaZaA/BitTorrent/eMule to download files. With effective management, IM/P2P can be a very good communication medium. However, P2P often consumes a huge amount of bandwidth. "Eat-all-you-can-eat" style of bandwidth consumption makes internal networks and external networks face the challenges. Bandwidth at external networks is occupied by P2P so mission-critical applications cannot obtain adequate bandwidth. Internal subscribers compete for the limited bandwidth at external networks, causing unfairness among the internal subscribers. For telecom operators and campus network administrators, simutaneously solving internal and external bandwidth problems becomes the most critical demand.

Organizations that emphasize network performance may have deployed L4 bandwidth management systems. BT / Xunlei / FlashGet / MSN / Yahoo / ICQ / AOL / Skype / Google Talk can emulate themselves to behave like web or email to cheat firewalls, tunnel through proxy servers, or even encrypt themselves with SSL. Network administrators cannot manage them completely.

7.1 Scenario

In order to manage the bandwidth of FTP, administrators hope to put FTP service into the **Middle** class and limit the **Middle** class to occupy only 18% of the inbound and outbound bandwidth individually.

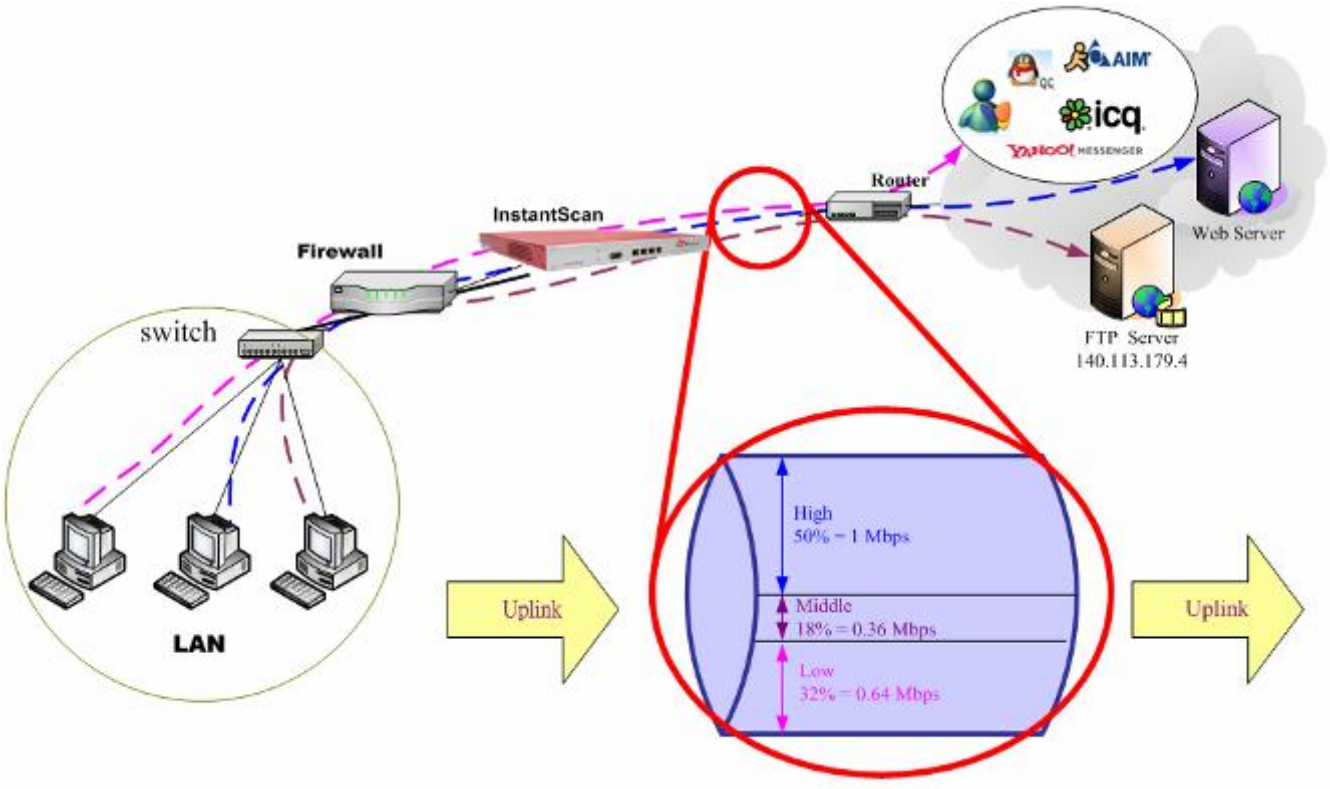


FIGURE 7-1 Outbound bandwidth management

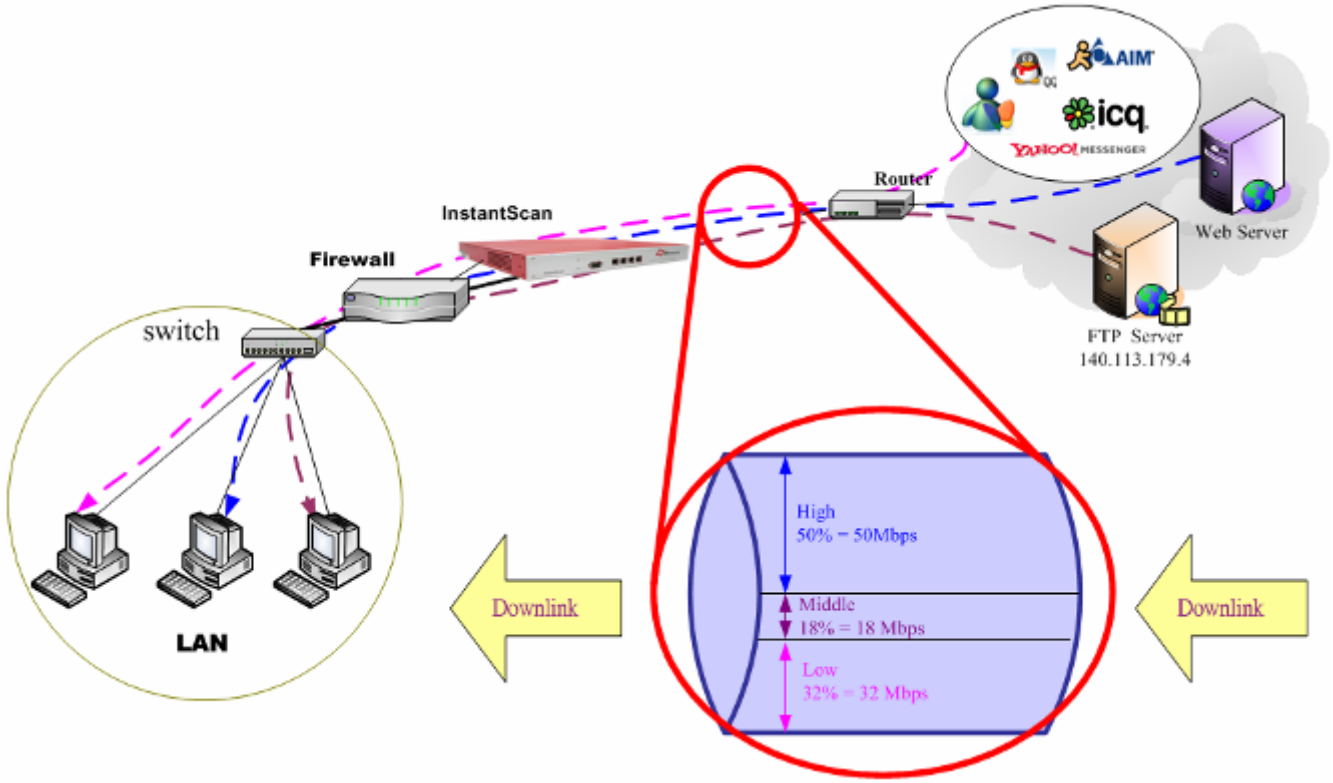


FIGURE 7-2 Inbound bandwidth management

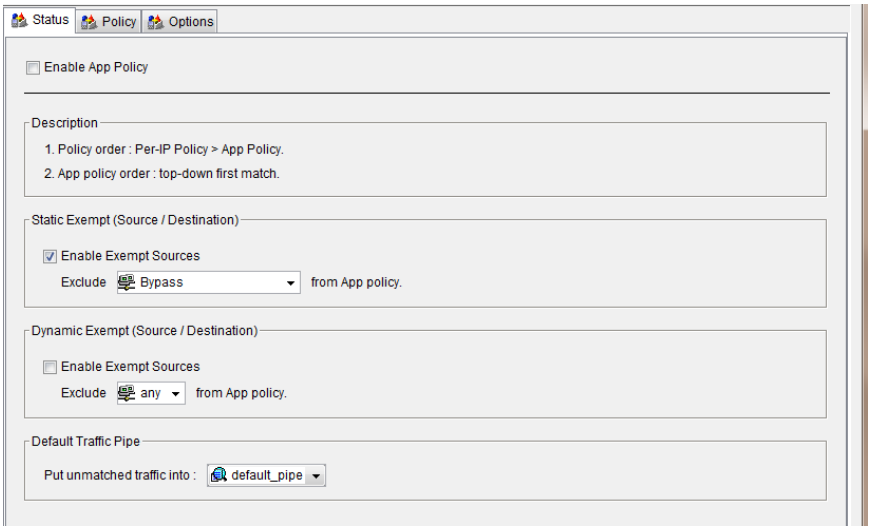
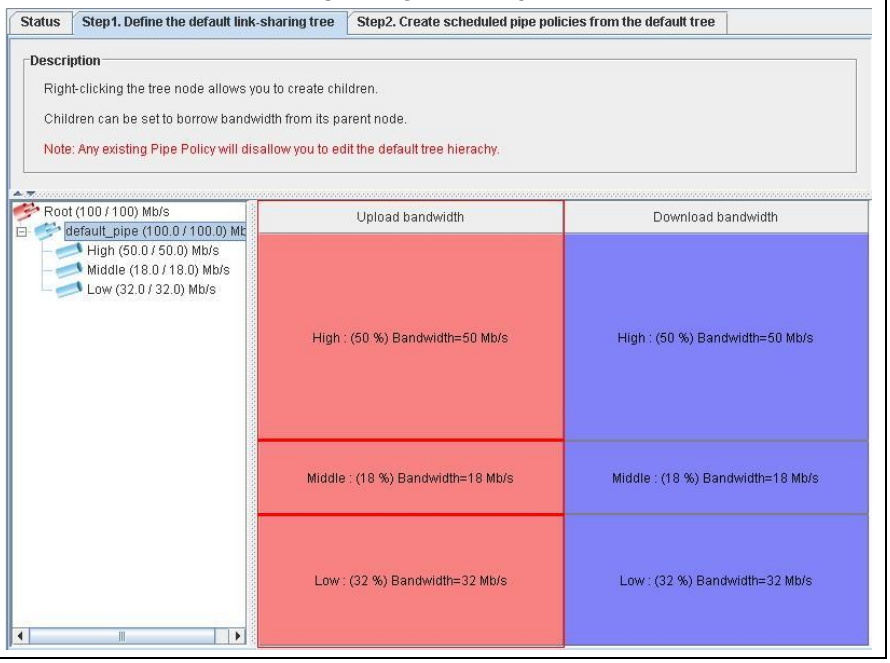
7.2 Methodology

The product can separate the inbound / outbound traffic into at least 3 classes as in the below Figure. The total bandwidth of the outbound traffic is 2Mbps, and the total inbound traffic is 100 Mbps.

Traffic direction	Total bandwidth	Class name	Parameters
Outbound	2 Mbps	High	50% = 1 Mbps
		Middle	18% = 0.36 Mbps
		Low	32% = 0.64 Mbps
Inbound	100 Mbps	High	50% = 50 Mbps
		Middle	18% = 18 Mbps
		Low	32% = 32 Mbps

According to the Figure, if some applications are classified into the class **Low**, the maximum outbound bandwidth will be 0.64 Mbps, and the maximum inbound bandwidth will be 32 Mbps. For example, if MSN/Yahoo/ICQ/AOL/GoogleTalk are classified into class Low, the bandwidth of MSN + Yahoo + ICQ + AOL + GoogleTalk + Webim will equal to 32 % of the outbound traffic (0.64 Mbps) or inbound traffic (32 Mbps).

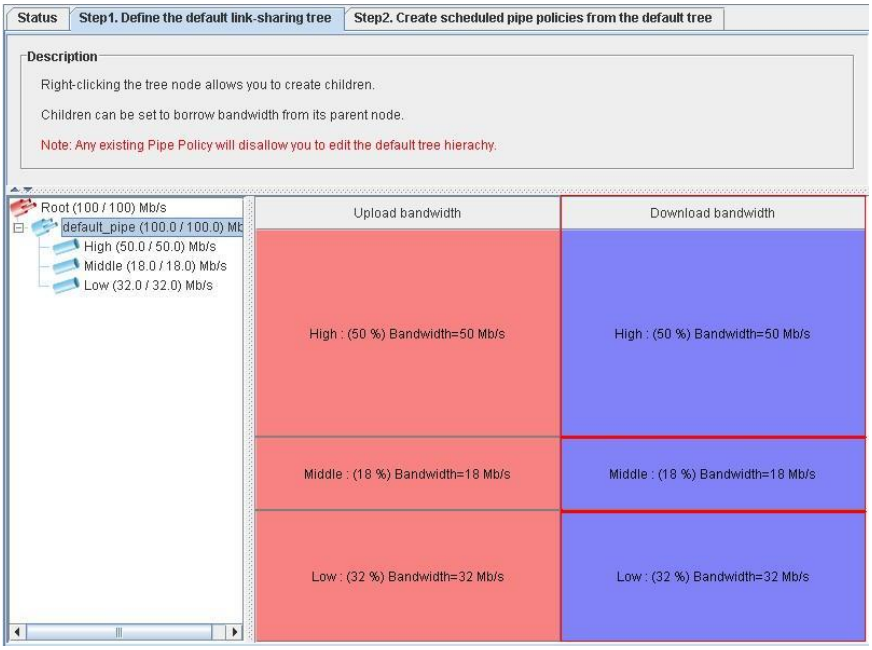
7.3 Steps

Step 1 **Start the Traffic Manager** Check the **Enable Traffic Management**.	**Functions > Traffic Manager > Traffic Manager** 
Step 2 **Setup outbound bandwidth** Input 2 at the **Outbound Traffic** field and then drag and drop the mouse for the bandwidth partitioning line. You can drag it to allow High to occupy 50% of the total bandwidth, Middle to occupy 18% of the total bandwidth, and Low to occupy 32% of the total bandwidth. During your dragging of the line, the exact number of the bandwidth will show up in the left fields.	**Functions > Traffic Manager > QoS Policy** 

Step 3 **Setup inbound traffic**

Input **100** at the **Inbound Traffic** field and then drag and drop the mouse for the bandwidth partitioning line. You can drag it to allow High to occupy 50% of the total bandwidth, Middle to occupy 18% of the total bandwidth, and Low to occupy 32% of the total bandwidth. During your dragging of the line, the exact number of the bandwidth will show up in the left fields.

Functions > Traffic Manager > QoS Policy



Step 4 **Enable App Policy**

Please check if the App Policy is enabled as in FigureFIGURE **7-1** and FIGURE **7-2**. After that, change the traffic profile of the FTP service to Middle and Allow in the security profile.

Functions > Traffic Manager > App Policy

Step 5 **Upload config**

Check the **Upload Configuration** item or click the icon  to upload the current configuration to the device.

Update > Upload Configuration

Chapter 8
App Policy

This chapter introduces how to conFigure the App Policy functions

8.1 Introduction to App Policy

Employees often use Outlook to receive emails, Internet Explorer to browse websites, Instant Messengers (IM) such as MSN/Skype to chat with friends, and P2P software such as BT / eDonkey / Xunlei / KaZaA / Kuro / ezPeer to download illegal data. Among them, Email and IM are the channel for information leakage or virus intrusion, while P2Ps are the bandwidth killers and may contain many spyware. What is worse, IM wastes employee's productivity by friends' interrupt during the office hours. However, IM can save communication cost and even make communications more efficient so that many enterprises are willing to allow IM.

Enterprises that emphasize network security may have deployed Email/Web auditing / management systems. In comparison, IM and P2P lack the auditing/recording/behavior management/content management/bandwidth management because IM/P2P software are optimized to tunnel through Firewalls. MSN / Yahoo / ICQ / AOL / Skype / Google Talk can tunnel themselves to behave like Web/ Email to cheat Firewalls, tunnel through proxy servers, or even encrypt themselves. Network administrators cannot manage them completely.

8.2 Scenario

1. CEO and CTO of the company should have full permission to access the Internet resources
2. Except for MSN, no other instant messenger software packages are allowed to use during office hours.
3. Besides Skype, there must be no other P2P applications during the office hours.
4. During the office hours, R&D members are not allowed to transfer files through Skype.

8.3 Methodology

1. Allow all traffic from CEO and CTO
2. Aside from CEO and CTO, employees can only use MSN. Other IMs are all blocked.
3. Aside from CEO and CTO, employees are allowed to use Skype, other P2P or VoIP software are strictly forbidden.
4. During the working hours, R&D members are not allowed to transfer files through Skype.

8.4 Steps

1. Enable the App Policy. Setup the scheduling of the working hours, and permit all traffic from the Boss group. Allow MSN but block all other IM software.
2. Allow Skype but deny all other P2P / VoIP software.
3. During the office hours, block R&D's Skype File Transfer activities.

Note:

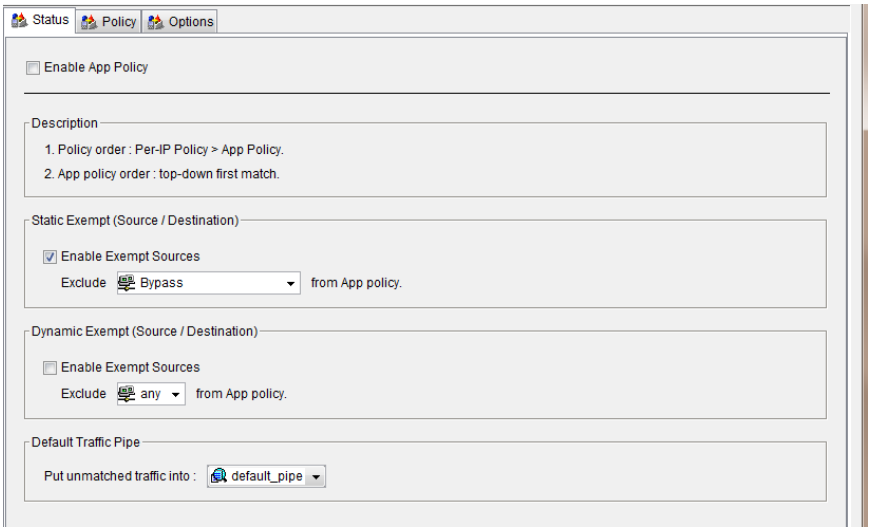
1. The default action of the device is Allow. So if you don't set it to block but leave it as allow, it is better to set it to never because that would greatly improve the throughput.
2. If the product is deployed outside the NAT / firewall, all the discovered traffic will be from the same IP address.

8.4.1 Setup IM Policy by App Policy Rules

Step 1 Enable the App Policy

Check the **Enable App Policy**.

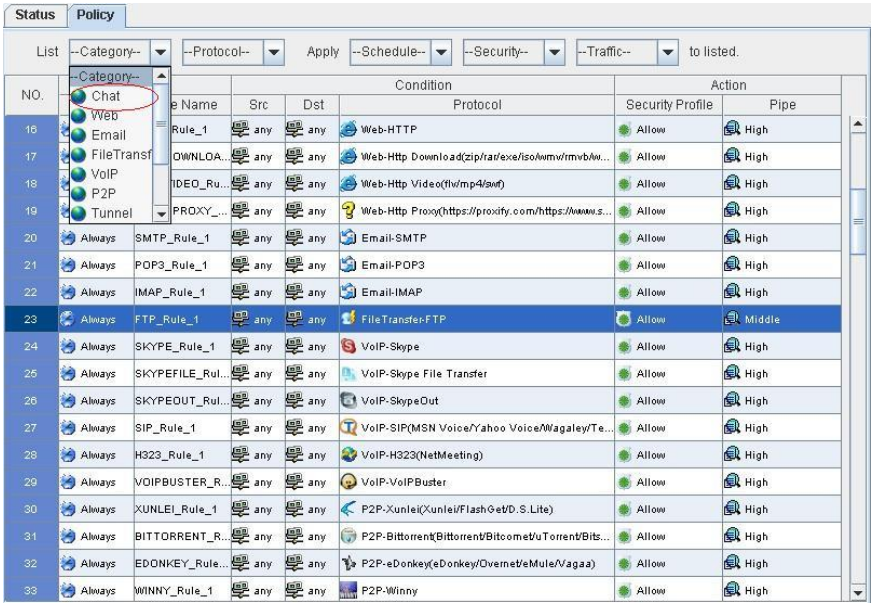
Function > Management > App Policy



Step 2 List the Chat Group

Select the **List Chat** in the search toolbar to list all rules regarding to the rules in Chat group.

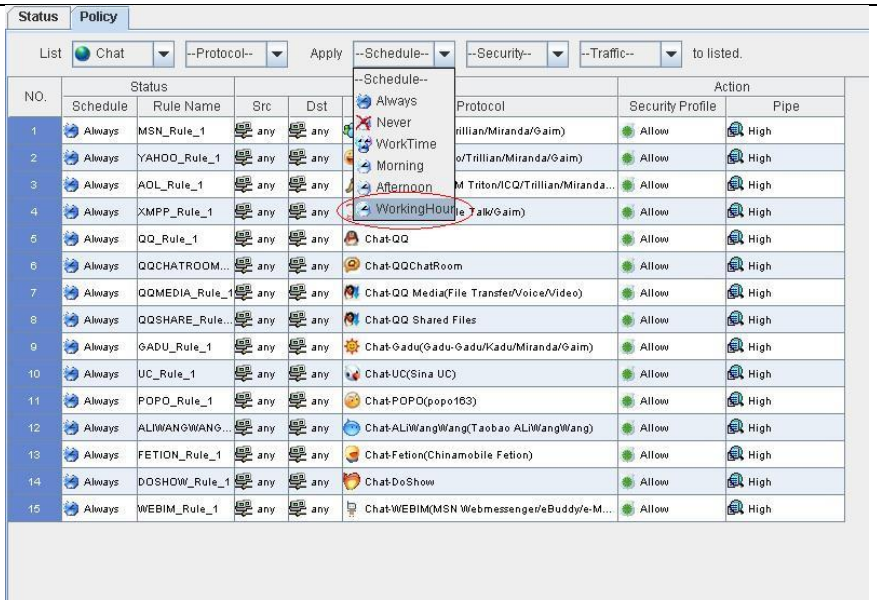
Function > Management > App Policy> policy



Step 3 Select the Schedule group

Select the **WorkingHours** schedule group to apply that schedule to all the rules regarding to the **Chat** group. You may also consider to manually select the schedule for individual applications.

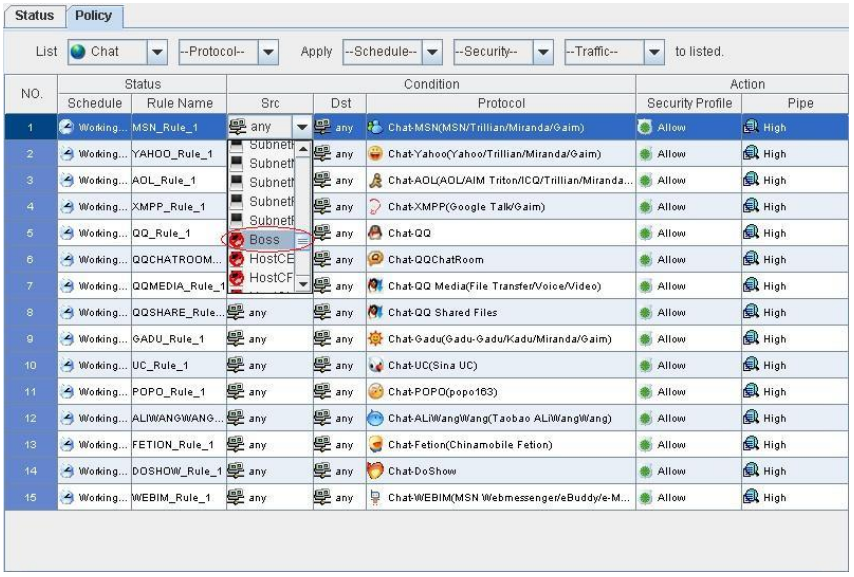
Function > Management > App Policy> policy



Step 4 Select the Source IP

CEO & CTO shoud has the complete permission to access the Internet. We have created a group **Boss (HostCEO, HostCTO)** in the last chapter. Selecting the the icon Boss means that all users except the Boss will apply to the App Policy rule.

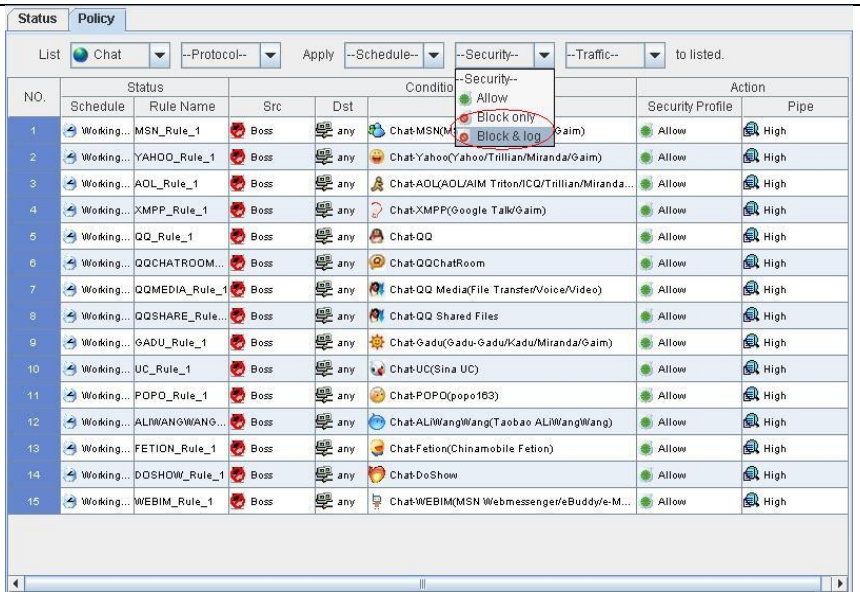
Function > Management > App Policy> policy



Step 5 Select the Security Profile

Select the **Block** in the **Security** listbox to apply the block policy to all listed **Chat** applications. Subsequently, remember to choose **Allow** at the MSN policy rule since the company allows MSN during office hours.

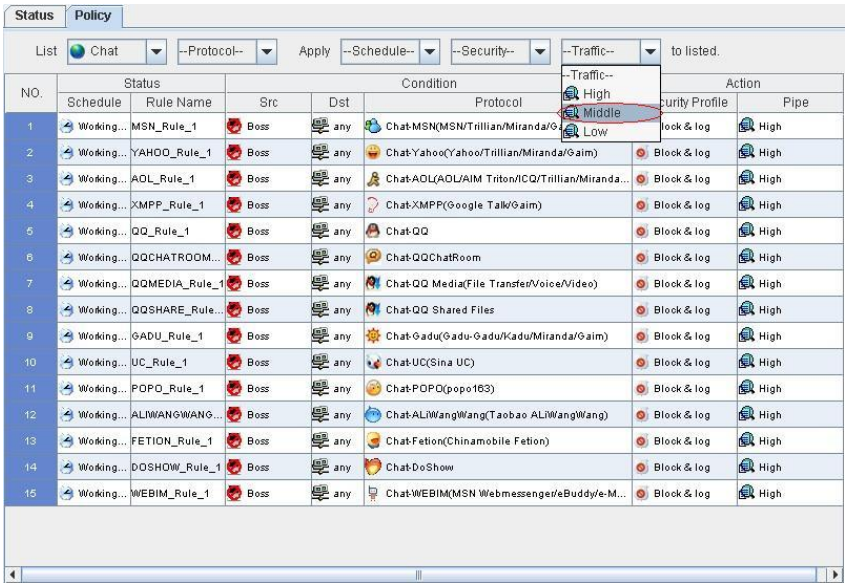
Function > Management > App Policy> policy



Step 6 Select the Traffic Profile

Select the **Middle** in the **Traffic** listbox to apply the middle bandwidth policy to all listed **Chat** applications.

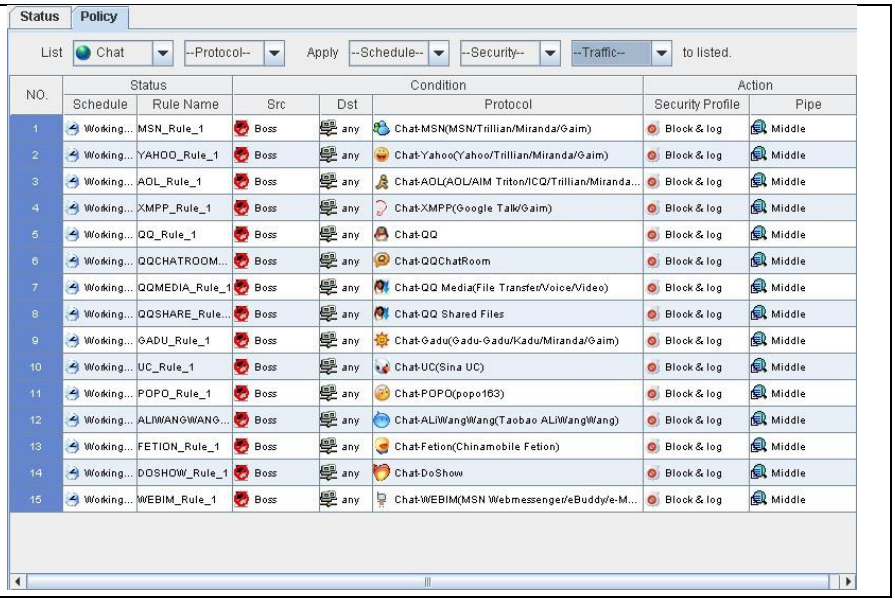
Function > Management > App Policy> policy



Step 7 Browse the policy

Browse the Chat policy rules to make sure that all your settings are properly set.

Function > Management > App Policy> policy



Field		Description	Range / Format	Example
List	Category	List all policy rules whose category field contains the selected category item	Pre-defined items	Chat
Apply _____ to listed.	Schedule	List all policy rules whose schedule field contains the selected schedule item	User-defined items	WorkingHours
	Security Profile	List all policy rules whose security field contains the selected security item	Allow / Block	Block
	Traffic Profile	List all policy rules whose traffic field contains the selected bandwidth item	High / Middle / Low	Middle

FIGURE 8-1 Quick configuration toolbar for App Policy

Field	Description	Range / Format	Example
Src	The internal IP address of the policy. Note that the icon Boss means inverse of the Boss address group.	Subnet / Range / Host	Boss
Dst	The external IP address of the policy. Note that the icon Boss means inverse of the Boss address group.	Subnet / Range / Host	any
Protocol	The applications of the passing traffic to be managed.	Pre-defined	Chat-MSN
Security Profile	Action of the policy: allow or block.	Allow / Block	Allow
Traffic Profile	Action of the policy: the bandwidth class the traffic belongs to.	High / Middle / Low	Middle

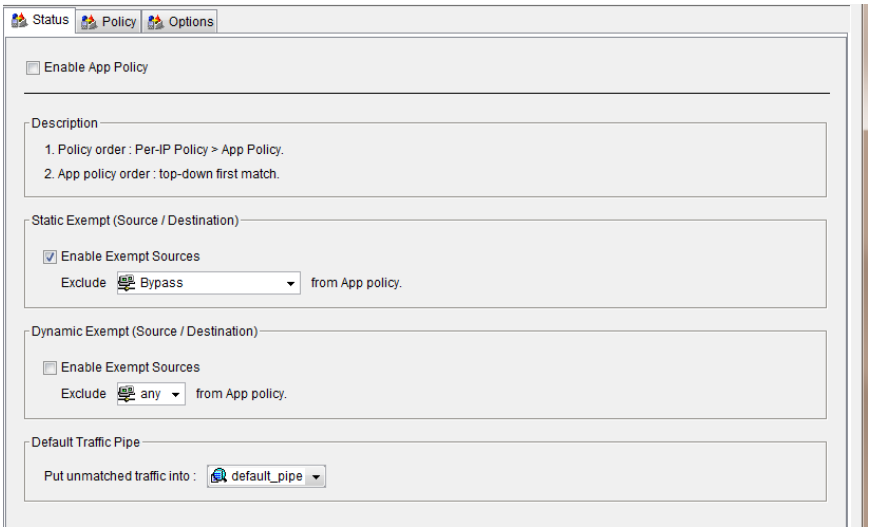
Figure 8-2 Field description of the App Policy policy

8.4.2 Setup P2P policy by App Policy Rules

Step 1 Enable the App Policy

Check the **Enable App Policy**。

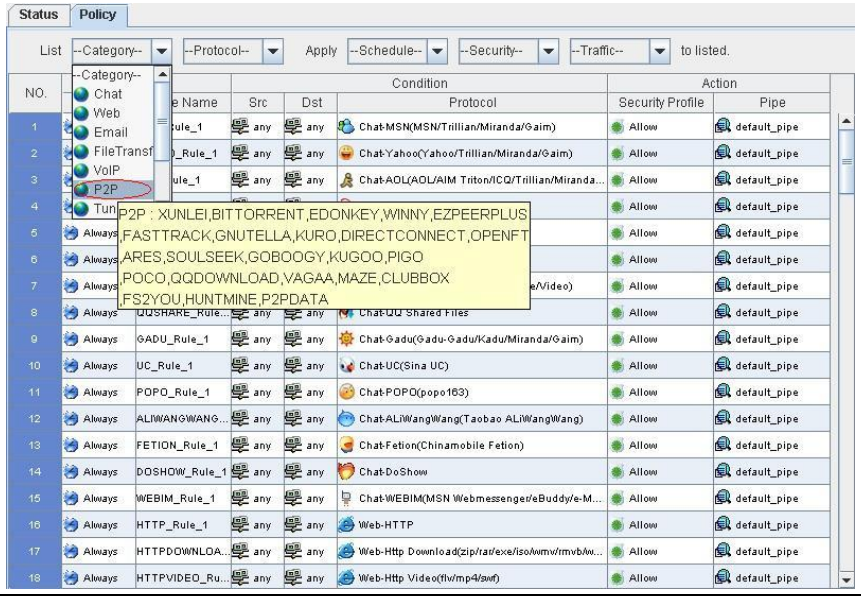
Functions > Traffic Manager > App Policy>Status



Step 2 List the P2P group

Select the **P2P** in the **Group** listbox as a filter to only show P2P policy rules.

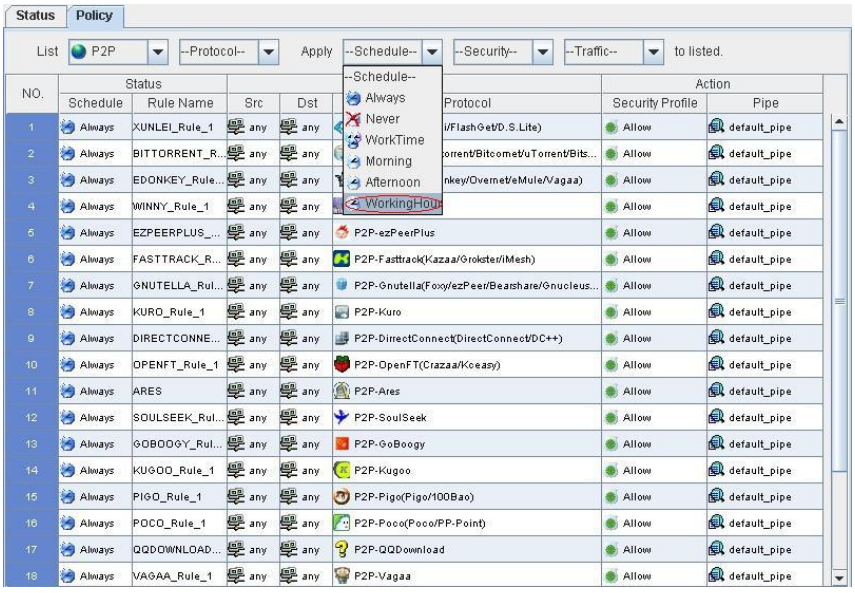
Functions > Content Manager > App Policy> policy



Step 3 Apply schedules to listed

Select the **WorkingHours** item in the Schedule listbox to apply the selected schedule to all listed policy rules. You can also select the item in each policy rule.

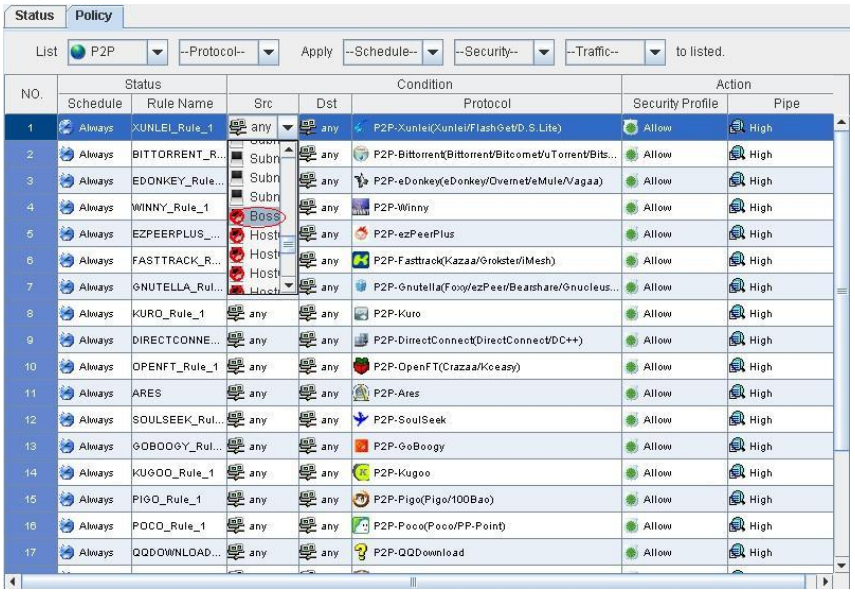
Functions > Content Manager > App Policy> policy



Step 4 Select source IP

Since CEO and CTO has full permission to access the internet resource, we use the group **Boss (HostCEO, HostCTO)** created in the last chapter. We select the the Icon Boss to apply all users to the App Policy except the group **Boss.**

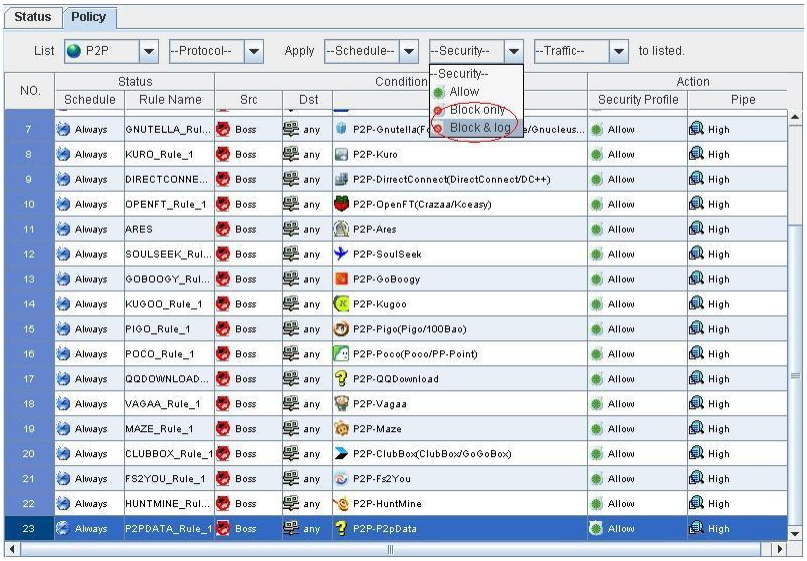
Functions > Content Manager > App Policy> policy



Step 5 Select security profile

On the toolbar of **Secuirty Profile**, select the **Block** to block all P2P applications.

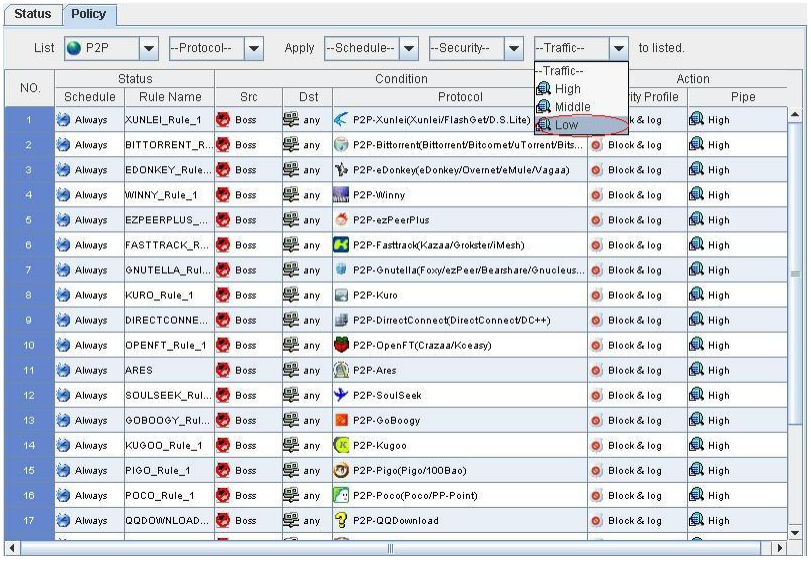
Functions > Content Manager > App Policy> policy



Step 6 Select traffic profile

On the toolbar of the Traffic Profile, select the profile **Low** to the P2P category to limit all P2P traffic in the traffic pipe **Low**.

Functions > Content Manager > App Policy> policy

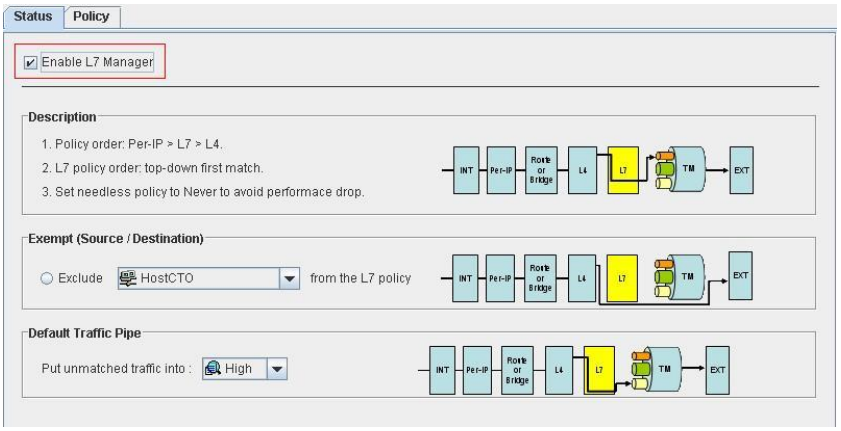


8.4.3 Setup VoIP policy by App Policy Rules

Step 1 Enable the App Policy

Check the **Enable App Policy**.

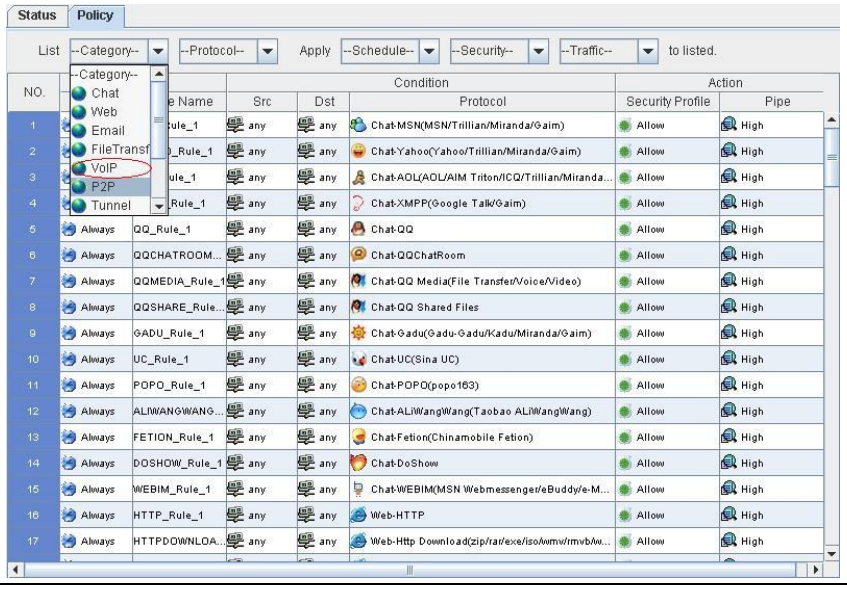
Functions > Content Manager > App Policy>Status



Step 2 List VoIP group

Select the **VoIP** in the List field, then all VoIP policy rules will be displayed on the screen.

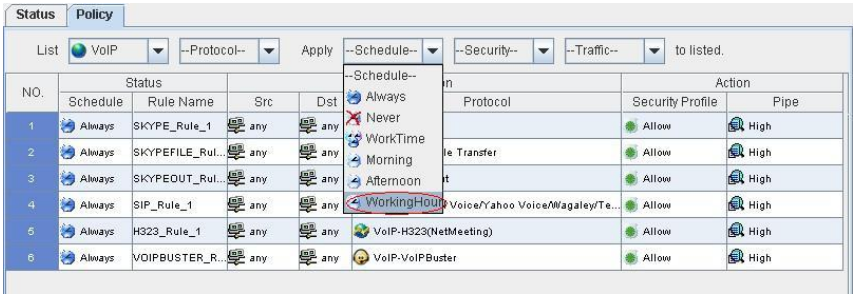
Functions > Content Manager > App Policy> policy



Step 3 Choose schedule

On the quick configuration toolbar, select the **WorkingHours** item in the **Apply** field. All the listed policy rules will be set to the same schedule. Of course, you can setup each rule one by one, too.

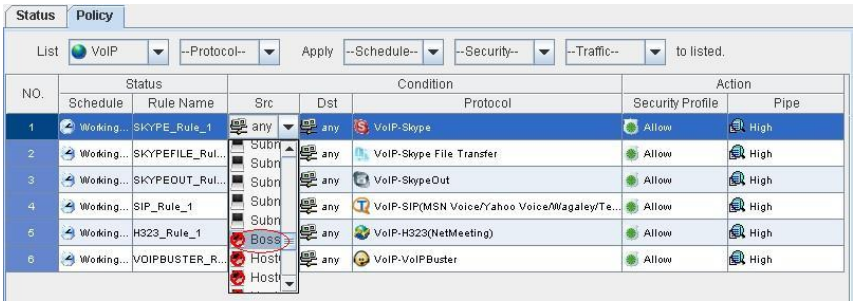
Functions > Content Manager > App Policy> policy



Step 4 Choose source IP

Since CEO & CTO should have full permission to access the Internet resources, we can assign the address object **Boss** setup in the last chapter to exclude them from being managed. Select the Icon Boss to exclude them.

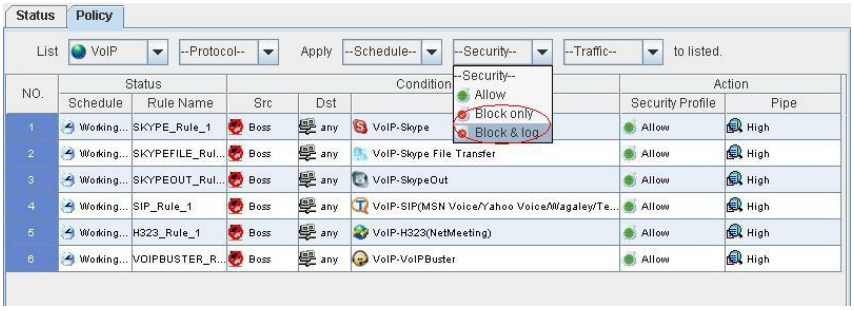
Functions > Content Manager > App Policy> policy



Step 5 Choose security profile

In the quick configuration toolbar, select **Block** to apply Deny policy to all listed rules.

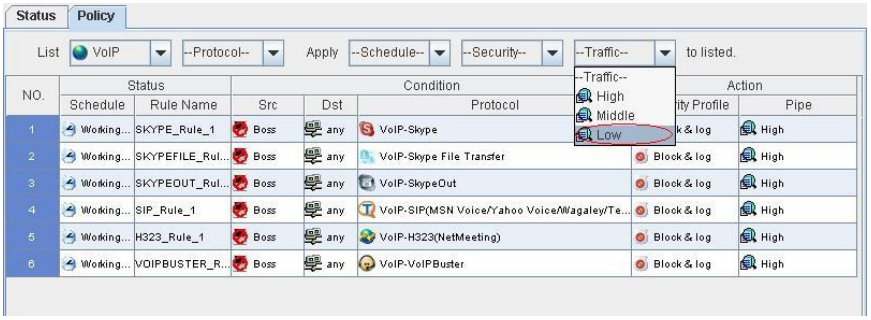
Functions > Content Manager > App Policy> policy



Step 6 Choose the bandwidth class

In the quick configuration toolbar, select **Low** at the **Traffic Profile** field to limit all P2P applications in the **Low** traffic pipe.

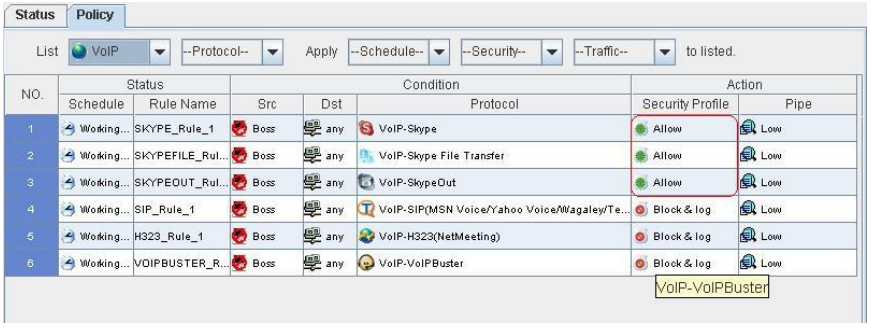
Functions > Content Manager > App Policy> policy



Step 7 Adjust security profile of Skype

According the policy of the company, we allow the employees to use Skype. So you have to adjust the security profile of Skype to the **Allow** state. In this way, the Skype traffic can pass through the product.

Functions > Content Manager > App Policy> policy



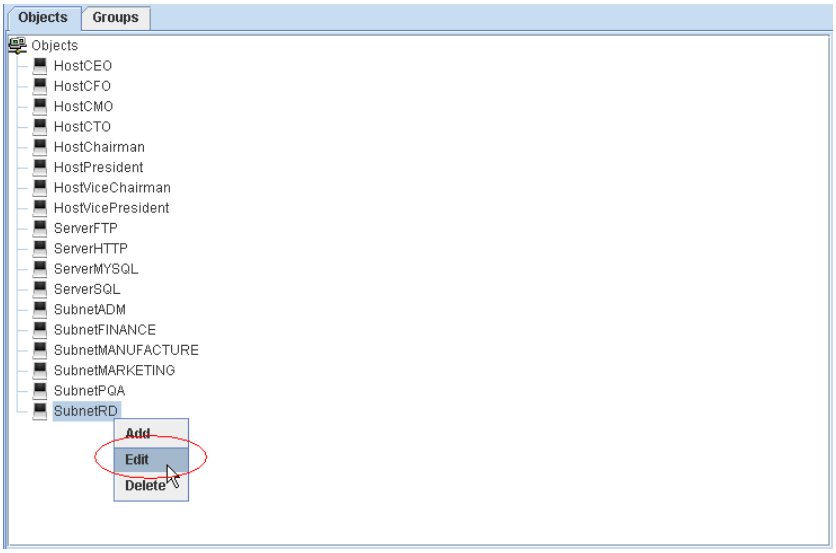
8.4.4 Blocking "VoIP - Skype File Transfer"

Step 1 Edit the Object Manager

Since the R&D department is not allowed to use Skype File Transfer, we must include the IP address of the R&D department (192.168.17.1 ~ 192.168.17.254).

Right click the SubnetRD and select the **Edit** Button.

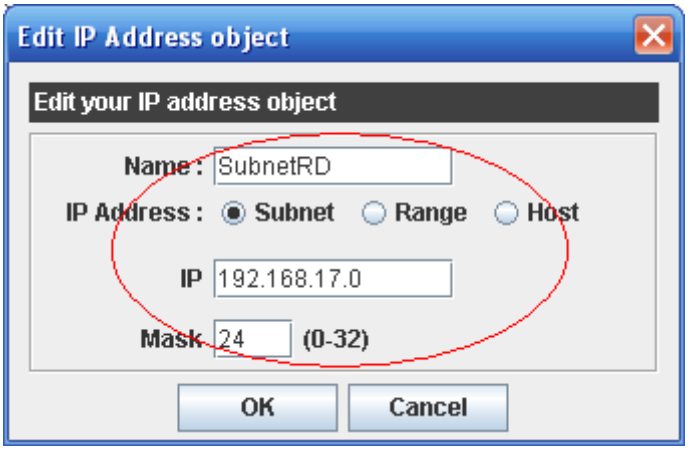
Functions > Content Manager > Object Manager > Address > Objects



Step 2 Setup the IP of the R&D

The address object can be a subnet, range, or host. We can setup the SubnetRD to be a range object of 192.168.17.1-192.168.17.254 or a subnet object of 192.168.17.0/24. Click the **OK** button to finish the setting.

Functions > Content Manager > Object Manager > Address > Objects

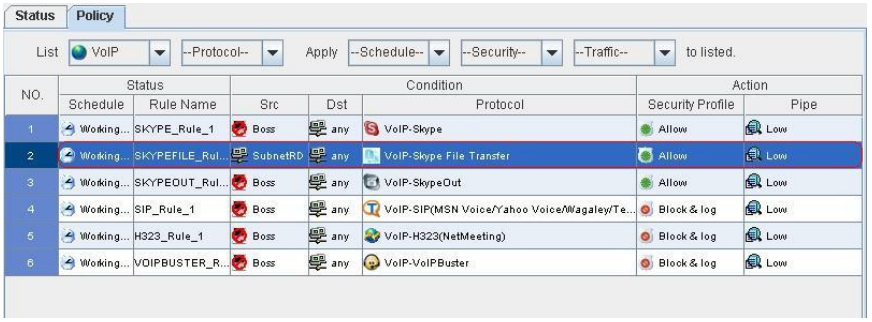


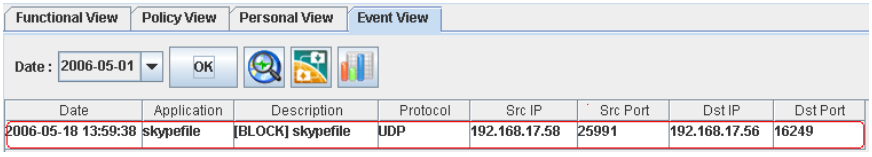
Step 3 Block Skype File Transfer of RD during office hour

According to the company's policy, all VoIP software packages are blocked except the Skype. However, all R&D members are not allowed to transfer files through Skype during office hours.

In the last chapter we have setup the rules for the VoIP. Now we need to adjust the policy. Click the **VoIP-Skype File Transfer** and select the **SubnetRD** option, and then select the **Block** at the security profile field.

Functions > Content Manager > App Policy



Step 4 Upload config Check the **Upload Configuration** item or click the icon  to upload the current configuration to the device.	**Update > Upload Configuration** 
Step 5 Skype File Events From the right figure we can see that the RD whose IP is 192.168.17.58 attemps to use Skype to transfer files. However, it was blocked by the product.	**Functions > Reports > App Policy > Event View** 

Tips:

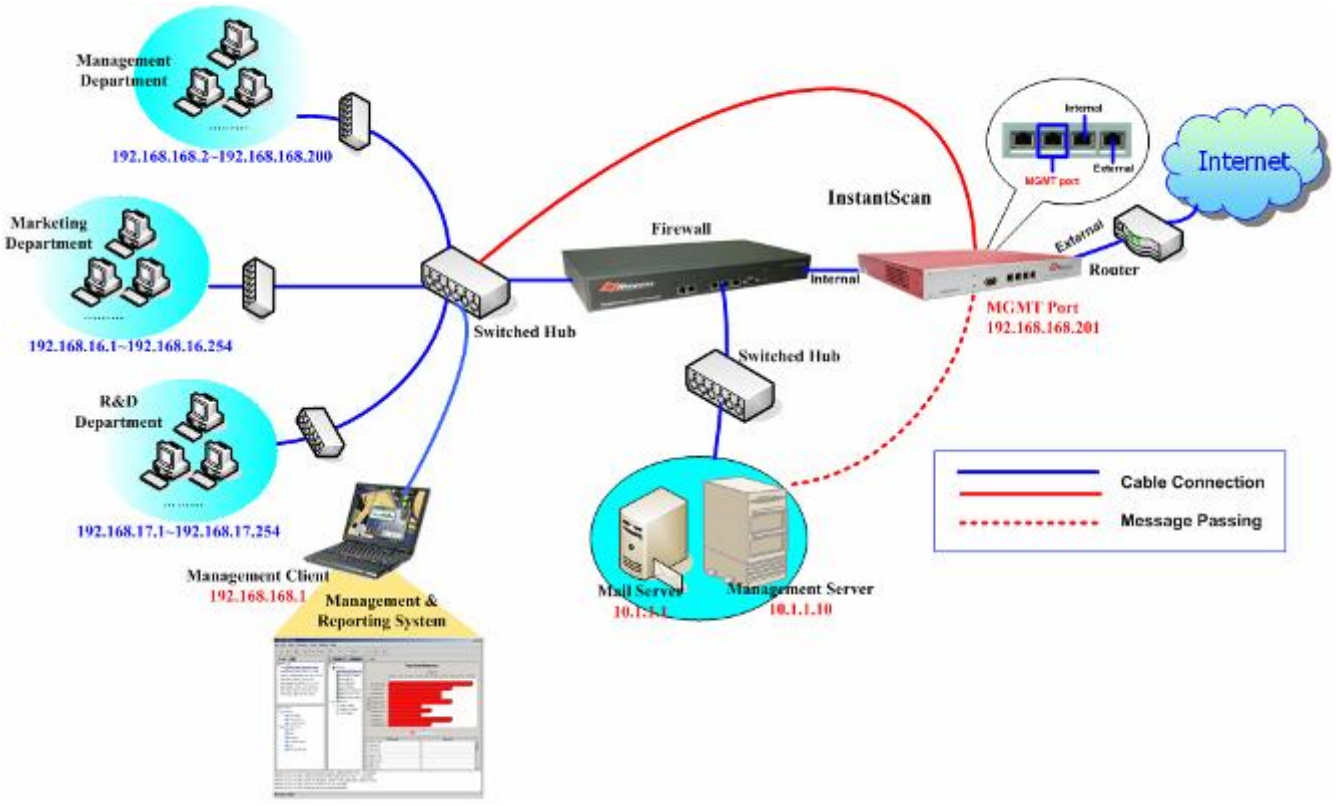
1. If you want to select or deselect some rule, you can use **<Ctrl> + <left click>** to adjust the selected policy rules.
2. If the background color of some rule appears as light yellow, it means that you have already selected the rule. If you want to quickly adjust settings to all the selected rules, just select the appropriate options in the toolbar. You can even drag & drop the mouse to select multiple rules at a time.

Chapter 9
Address & Schedule Objects

This chapter shows you how to setup objects for use with managing policy rules

9.1 Scenario

1. Company ABC hopes to manage all the permissions of all the IP address in the company. However, CEO & CTO has the complete permission to access all the Internet resources.
2. Company ABC's working hours are from Monday to Friday 8:30 to 17:30. 12:00-13:00 at noon is employee's free time to do anything. According to the company's policy, some IM or P2P applications are not allowed touse furing the office hours.
3. Objects of the same nature should be grouped together to facilitate the configuration of the policy rules.



9.2 Methodology

1. Assign CEO's IP address as 192.168.168.2 and CTO's IP address as 192.168.168.10. Then group CEO and CTO into a group object named boss.
2. Assign several timeslots of the company's office hours. Then group the timeslot schedule objects into a schedule group object named WorkingHours.

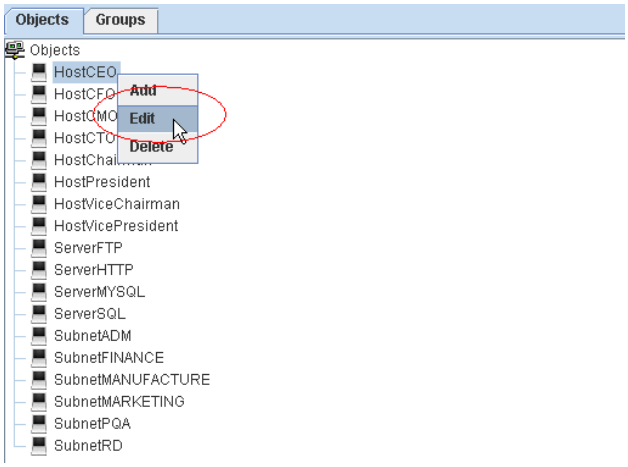
9.3 Steps

9.3.1 Address Settings

Step 1 Adding an address object

Right click on the item of **HostCEO**, and select **Edit**, you can start editing the content of the object. The product has already provided you several objects. You can edit them directly or delete them all.

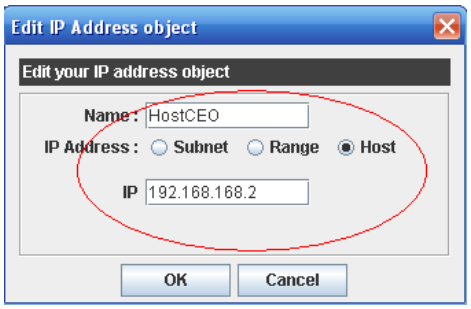
Function > Management > Object Manager > Address > Objects



Step 2 Editing the HostCEO object

Change the IP address of HostCEO into 192.168.168.2 if your CEO has an IP address of that.

Function > Management > Object Manager > Address > Objects



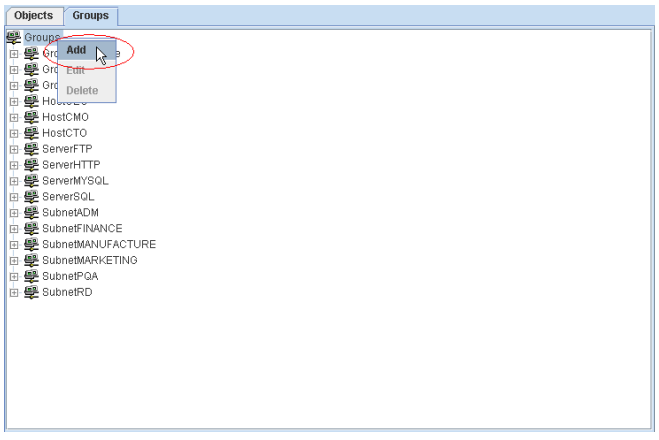
IP Address		Description	Range / Format	Example
Subnet	IP	IP address of the subnet	X.X.X.X	192.168.168.0
	Mask	Subnet mask	X.X.X.X	24
Range	Start IP	Starting IP of the address range object	X.X.X.X	192.168.168.1
	End IP	Ending IP of the address range object	X.X.X.X	192.168.168.10
Host	IP	IP address of an host address object	X.X.X.X	192.168.168.2

FIGURE 9-1 Definition of an address object

Step 6 **Adding object / group**

Right click on the group item and select the **Add** item.

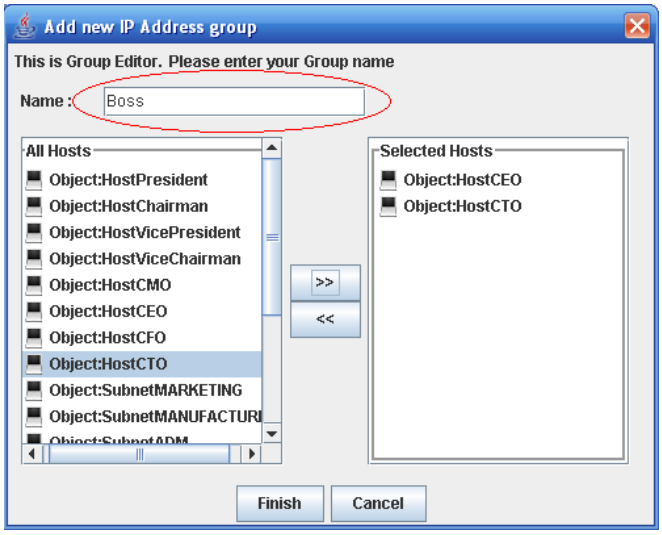
Function > Management > Object Manager > Address > Groups



Step 7 **Editing group**

Enter the name and select host objects from the left column. Click the **>>** to move the address object from the left to the right. If you want to remove some address objects from the current group, select the object in the right column and click the **<<** button. Click the **Finish** button to finish the settings.

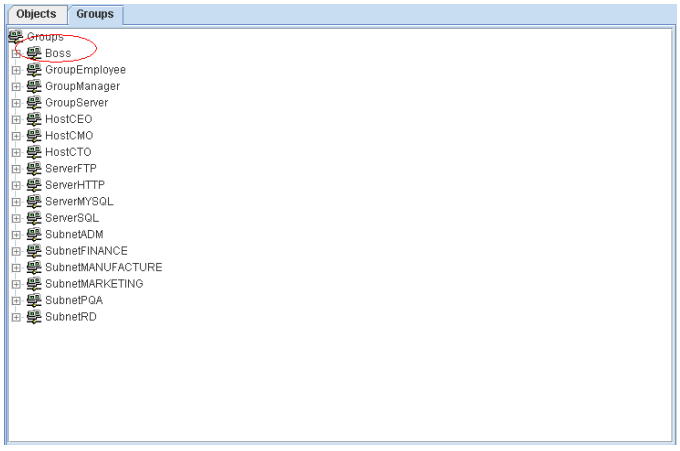
Function > Management > Object Manager > Address > Groups



Step 8 **Display existing address groups**

After you click the **Finish** button, all groups will be shown on the screen.

Function > Management > Object Manager > Address > Groups



Step 9 **Upload config to the device**

Check the **Upload Configuration** item or click the icon  to upload the current configuration to the device.

Update > Upload Configuration

⚠ If some object is referred by some group or some policy rule, before you delete this object you have to delete the policy or group first. Otherwise, you will not be able to delete the object.

9.3.2 Schedule Control

Step 1 **Deleting the default schedule**

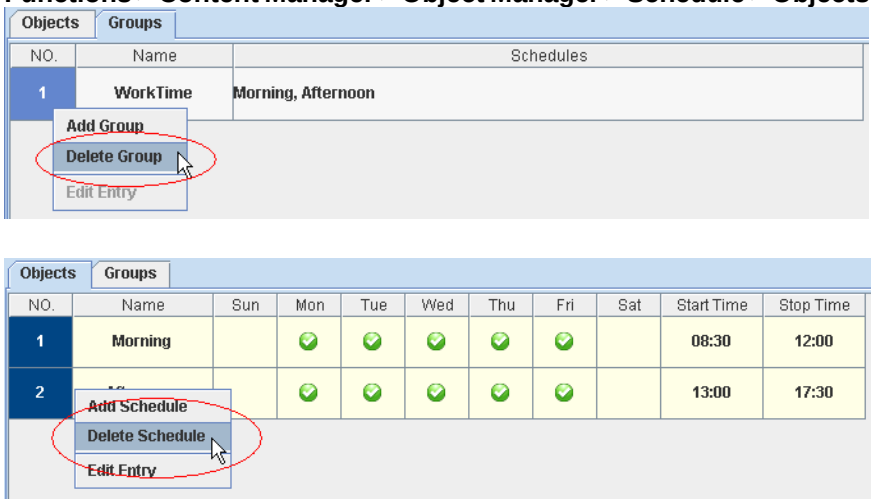
The product has provided two default schedules for you. If they cannot meet your needs, you can modify the schedule or delete it immediately.

In the following examples, we will delete default schedules and add a new schedule to demonstrate the process.

Note: Please note that before you can delete a schedule, you must make sure there is no rule referring to the schedule to be deleted.

The example at the top right one is to delete a group. You must delete the schedule inside the group so as to delete the whole group.

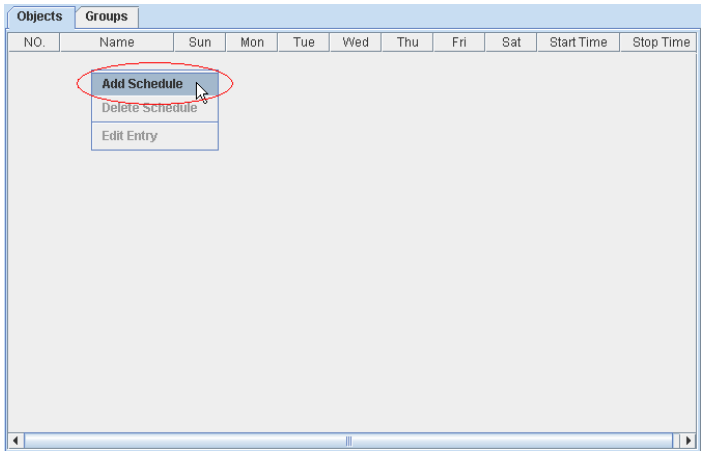
Functions > Content Manager > Object Manager > Schedule > Objects



Step 2 **Right click the schedule**

Right click at the schedule area and select the **Add Schedule** option.

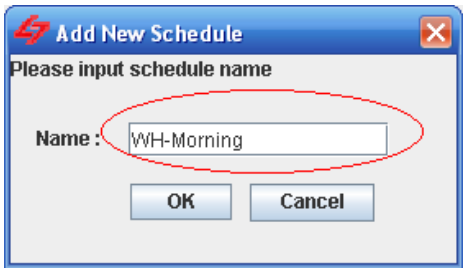
Functions > Content Manager > Object Manager > Schedule > Objects



Step 3 **Adding a new schedule**

Enter the name of the schedule. Click the **OK** button to close the dialog.

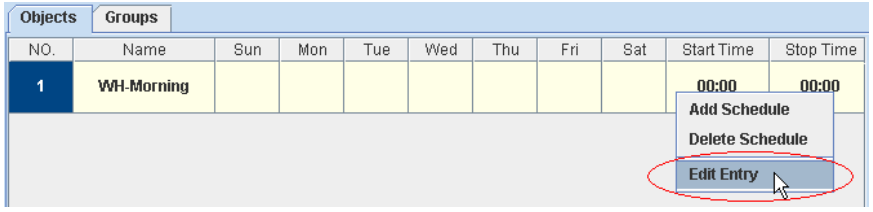
Functions > Content Manager > Object Manager > Schedule > Objects



Step 4 **Editing time**

Right click on the area of the WH-Morning rule and select the **Edit Entry** item.

Functions > Content Manager > Object Manager > Schedule > Objects

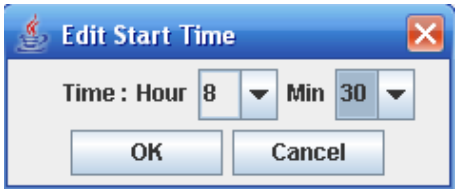


Step 5 **Pick the start time**

Select the **Start Time** and click the **OK** button to close the dialog.

The settings for **Stop Time** are the same.

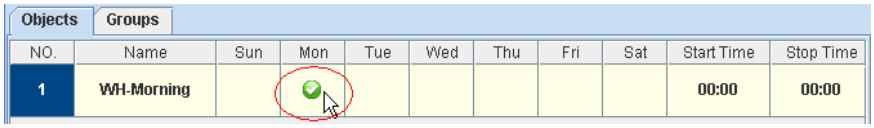
Functions > Content Manager > Object Manager > Schedule > Objects



Step 6 **Weekday schedules**

The office hours for company ABC are from Monday to Friday. Move your mouse over the area and click, you will get an icon like .

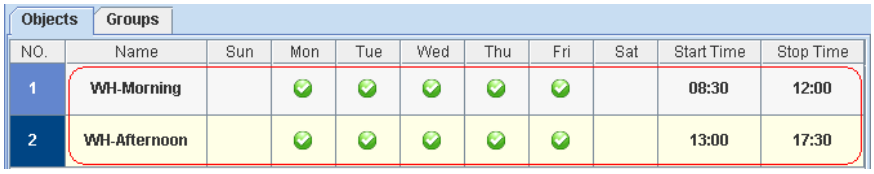
Functions > Content Manager > Object Manager > Schedule > Objects



Step 7 **Browse the results**

Now we have two schedule objects. We can start grouping them into a schedule group object.

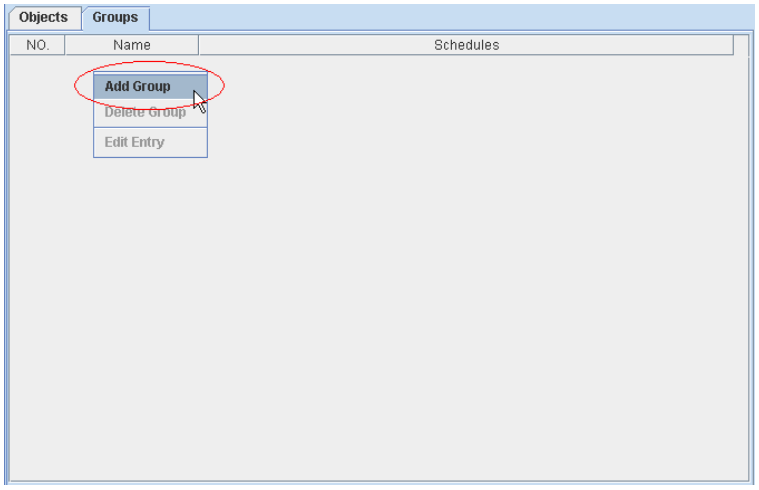
Functions > Content Manager > Object Manager > Schedule > Objects



Step 8 **Creating a new group**

Since the working hours for company ABC include 8:30~12:00 and 13:00~17:30, we have to group them into a group object so as to facilitate management of policy rules.Right click on the area and select the **Add Group** item.

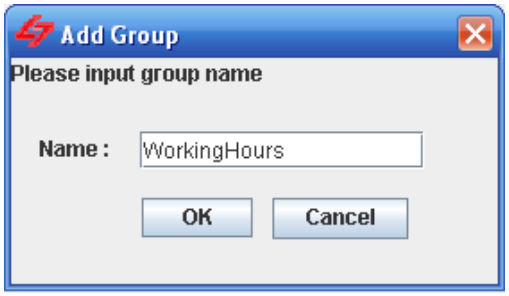
Functions > Content Manager > Object Manager > Schedule > Groups

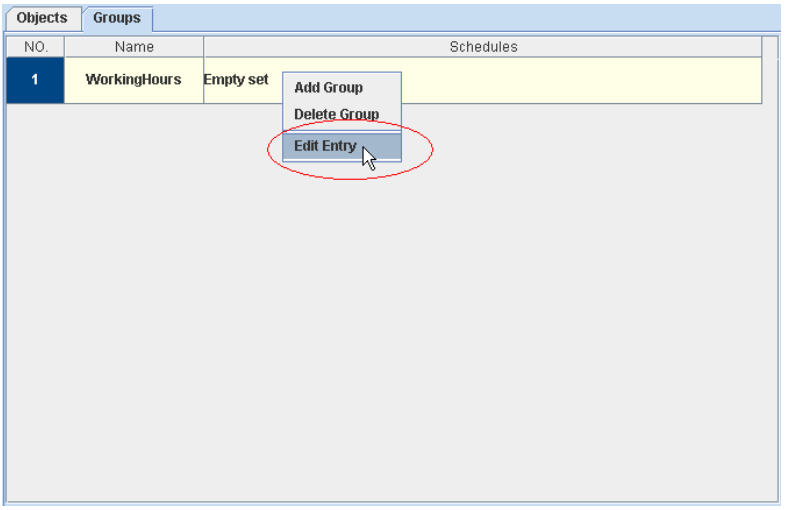
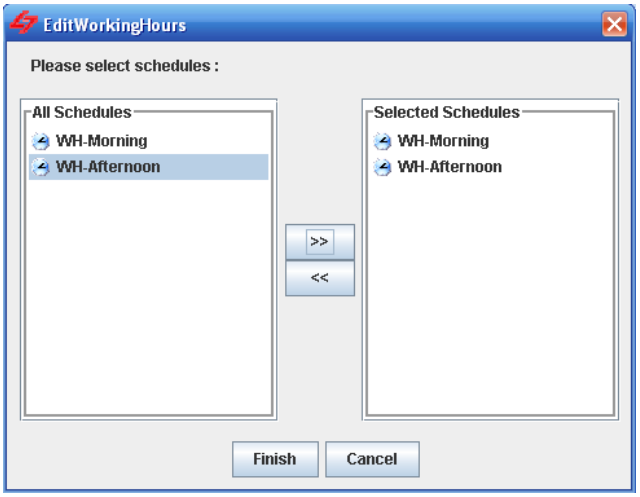
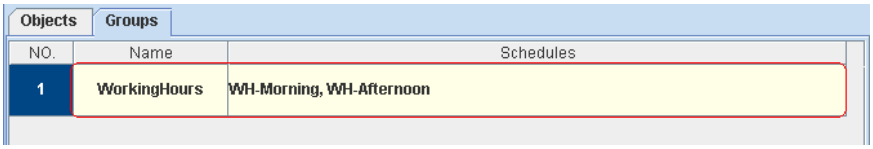


Step 9 **Input the group name**

Input the group name and click the **OK** button to continue.

Functions > Content Manager > Object Manager > Schedule > Groups



Step 10 **Open the schedule group** Right click on the schedule group object **WorkingHours** and select the **Edit Entry** item..	**Functions > Content Manager > Object Manager > Schedule > Groups** 
Step 11 **Edit the schedule group** Select schedules from the left column. Click the **>>** to move the schedule object from the left to the right. If you want to remove some schedule objects from the current group, select the object in the right column and click the **<<** button. Click the **Finish** button to finish the settings.	**Functions > Content Manager > Object Manager > Schedule > Groups** 
Step 12 **Display the current policy** After the settings, check your objects to see if your inputs are really updated to the screen.	**Functions > Content Manager > Object Manager > Schedule > Groups** 
Step 13 **Upload config** Check the **Upload Configuration** item or click the icon  to upload the current configuration to the device.	**Update > Upload Configuration**

⚠ **If some object is already used by some policy, you must chage or delete the policy before you can delete the object. Otherwise, you can never erase the object.**

Part 5

Content Manager

Chapter 10
Configure APP/Content with WebLogin

This chapter introduces how WebLogin gets users' identity for policy enforcement in APP/Content

10.1 Scenario

Enterprieses often require to authenticate users to know the exact identity of each users. The Web Login function in the product can achieve this by the following steps:

1. Force the subnet of R&D employees to authenticate by web login. Non-login users are not allowed.
2. Make the reports tagged with the authenticated Web Login user names.
3. Configure APP/Content policy rules to use the Web Login user names

10.2 Methodology

1.1 All members should authenticate every 8 hours except the boss.
- 1.1.1 Enable Web Login
- 1.1.2 Add Web Login user names and password
- 1.1.3 Add Web Login rules

1.2 Setup rules using Web Login names for filtering
- 1.2.1 Assign Web Login user names in App Policy rules
- 1.2.2 Assign Web Login user names in Content policy rules
- 1.2.3 Import Web Login user accounts into content policy rules

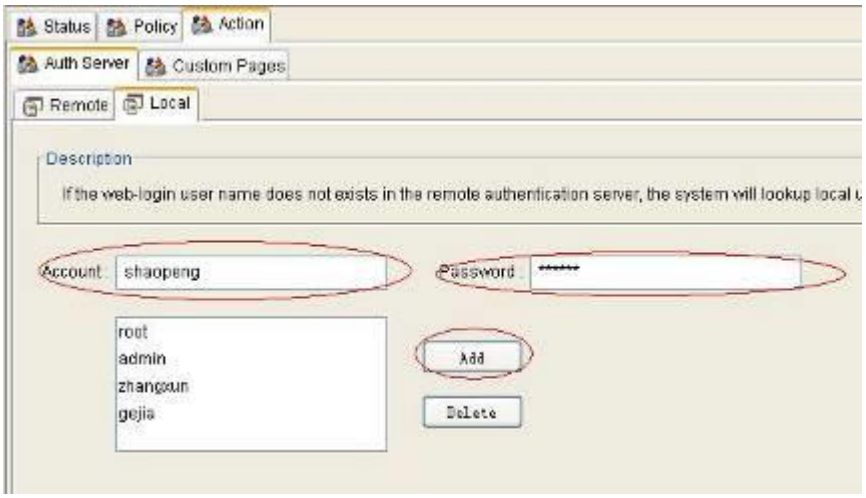
10.3 Steps

10.3.1 All members are required to login via captive portal page every 8 hours except the boss.

10.3.1.1 Enable Web Login

Step 1 Enable Web Login Click the Web login > status, Select the **Enable Web login** · and upload the configuration.	**Functions >Object Manager > Web Login > Status**  (圖 1)

10.3.1.2 Add Web Login user names and password

Step 1 Add a Web Login account and its password In the Account field, fill in the account name and its password and then press the Add button, the account will then be added into the system. Upload the configuration.	**Functions >Object Manager > Web Login > Action > Local**  (圖 1)

You can also use remote authentication with POP3(s) / IMAP(s) / RADIUS / LDAP servers. Below are parameters for each authentication method:

POP3 Fields	Description	Example
Server IP	Pop3(s) server IP address	10.1.1.1
Server Port	Pop3(s) port number. Usually POP3 is 110 and POP3S is 995.	110
Encryption	SSL is a stand encryption protocol. POP3's SSL version is call POP3S; IMAP's SSL version is called IMAPS.	Disable

IMAP Fields	Description	Example
Server IP	IMAP(s) server IP address	10.1.1.1
Server Port	Pop3(s) port number. Usually POP3 is 143 and POP3S is 993.	993
Encryption	SSL is a stand encryption protocol. POP3's SSL version is call POP3S; IMAP's SSL version is called IMAPS.	Enable

Radius Fields	Description	Example
Server IP	Radius server IP address	10.1.1.2
Server Port	Radisu server connection port	1812
Secret	Secret is a encryption key of a Radus server. All communication peers share a key to encrypt traffic or do authentication.	secret

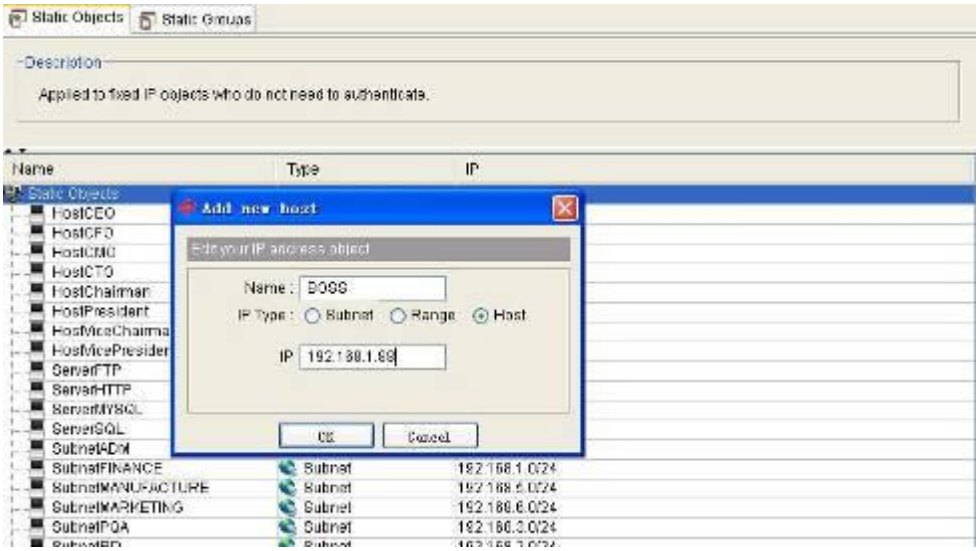
LDAP Fields	Description	Example
Server IP	LDAP server IP address	10.1.1.11

10.3.1.3 Add Web Login rules

Step 1 Add Static Object "BOSS"

Since the BOSS is not required to authenticate, we first setup his/her IP address in the static object. Right click on any icon in this page and select **Add a new host**. Fill in his/her IP address and click the OK button.

Functions >Object Manager > Static > Address > Static Object

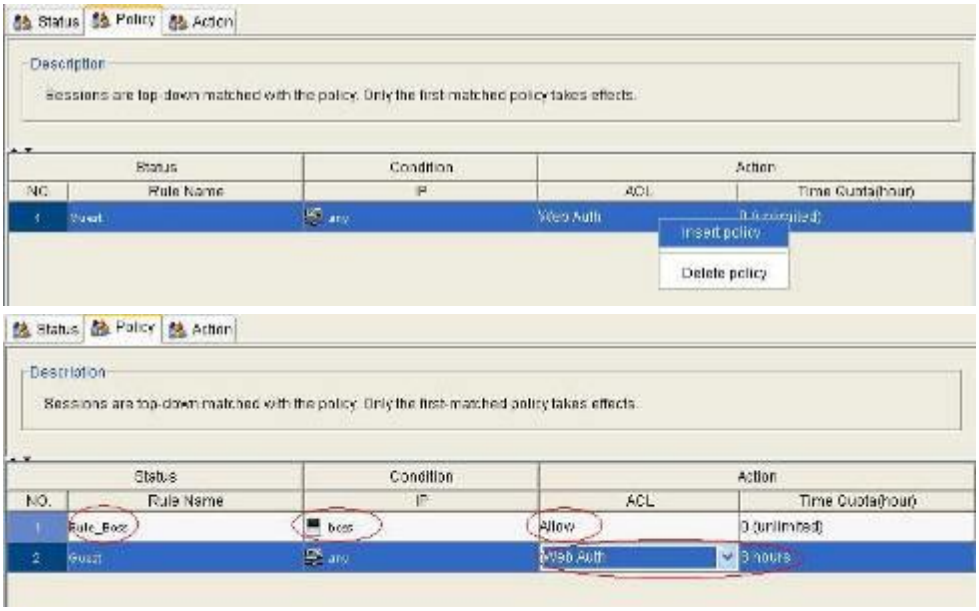


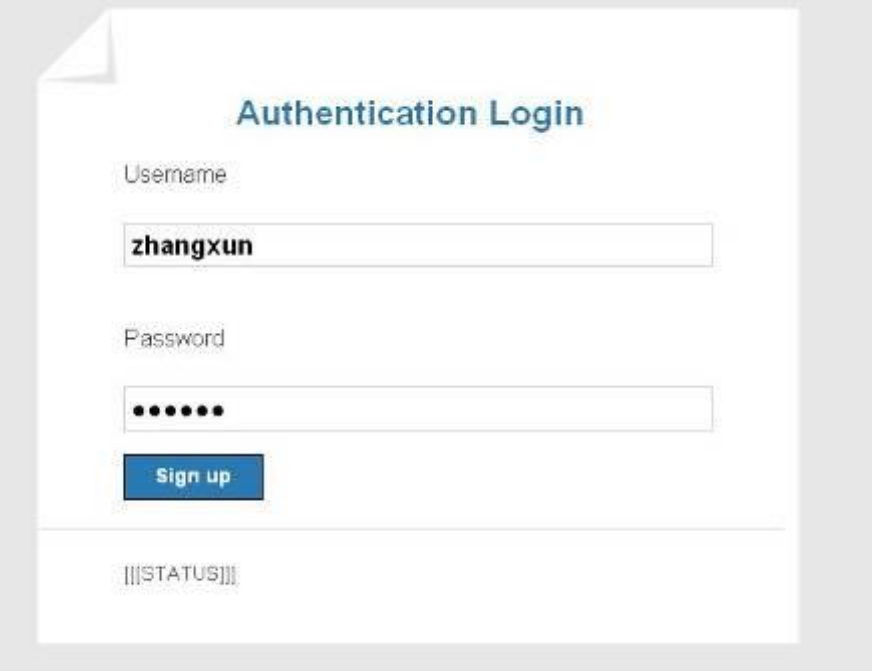
Step 2 Add Web Login rules

In the Policy tab, there is a default rule "Guest". This rule applies to all users. We want to exclude BOSS for Web Login in the following setup:

Right click on the policy area and click the **Insert policy** to insert a new policy named rule_BOSS, and select the object **BOSS** in the IP address field. Choose **Allow** at the ACL field.

Select the "Guest" policy rule and choose **Web Auth** at the ACL field, and double click the System Logout field to enter 8 hours. Click the **OK** button and then upload the configuration.

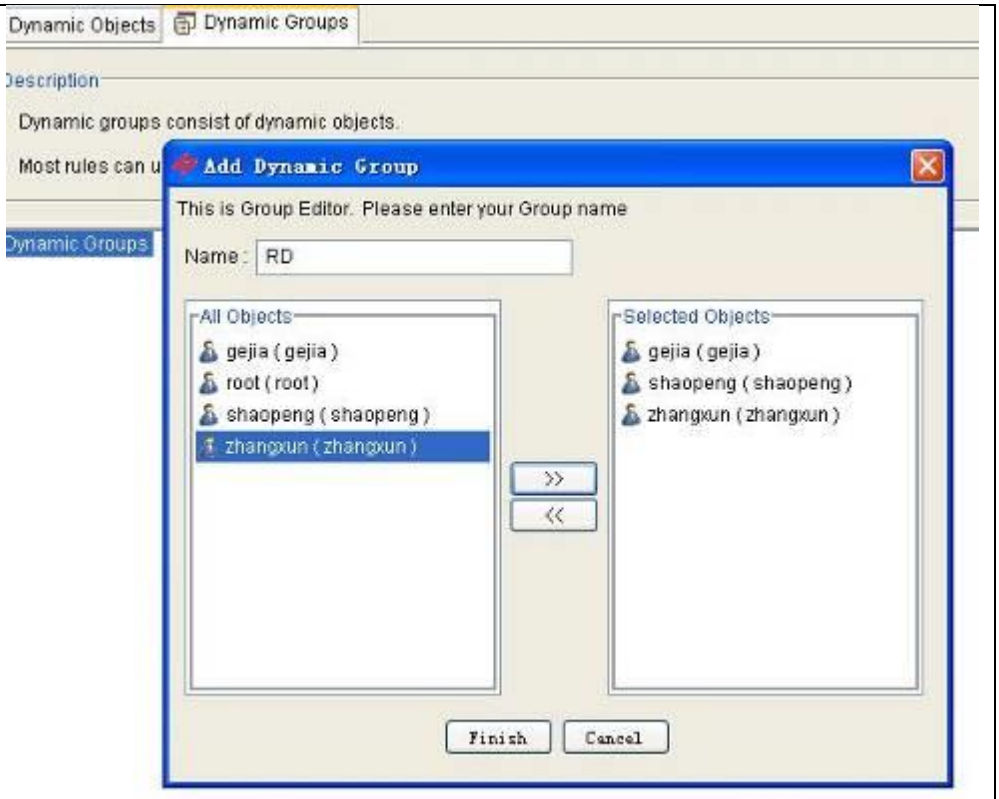


Step 3 Input account names At employees' PCs, when they open a browser and connect to somewhere, their browsers will be redfirected to the Web Login page. Employees are required to ask for user names and passwords from IT managers to login to the network.	

10.3.2 Match rules using Web Login account names

10.3.2.1 Assign Web Login account names in App Policy rules

Step 1 Add Web Login accounts In Dynamie Objects, add the accounts that are needed to authenticate, such as shaopeng, zhangxun, gejia, root (Fig.1). We can also group the above accounts into a group, such RD (Fig.2). Upload the configuration.	**Functions > Dynamic > Dynamic Objects**  (Fig.1) **Functions > Dynamic > Dynamic Groups**

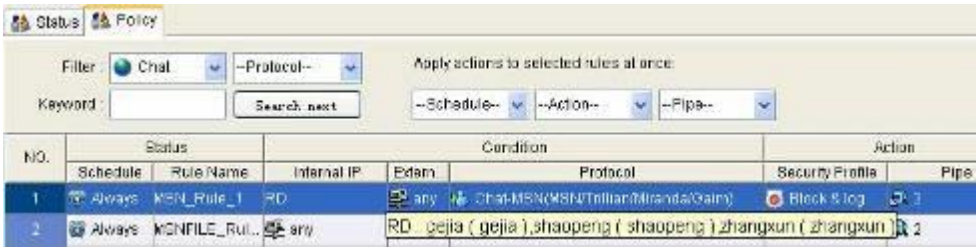


(Fig.2)

Step 2 Assign Web Login names in APP rules

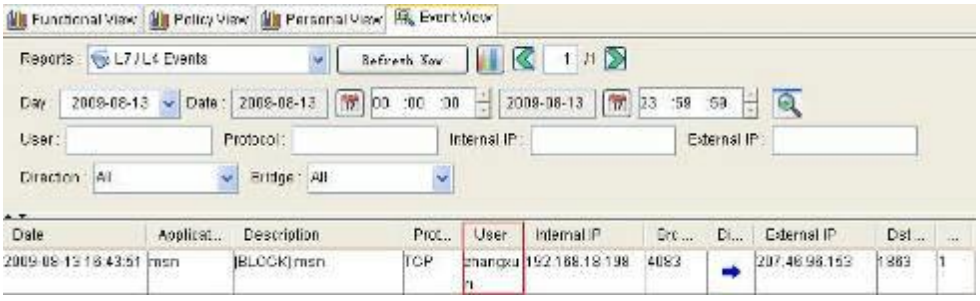
We can assign the objects / groups in the dymanic objects to any App Policy rules. For example, we don't want the group RD to use MSN, we can assign the group RD in the MSN policy rule. Upload the configuration. We can see that zhangxun belonging to the list of MSN has been blocked and logged.

Functions >Traffic Manager > L7 Policy > Policy



(Fig. 1)

Functions >Reports > Traffic-APP

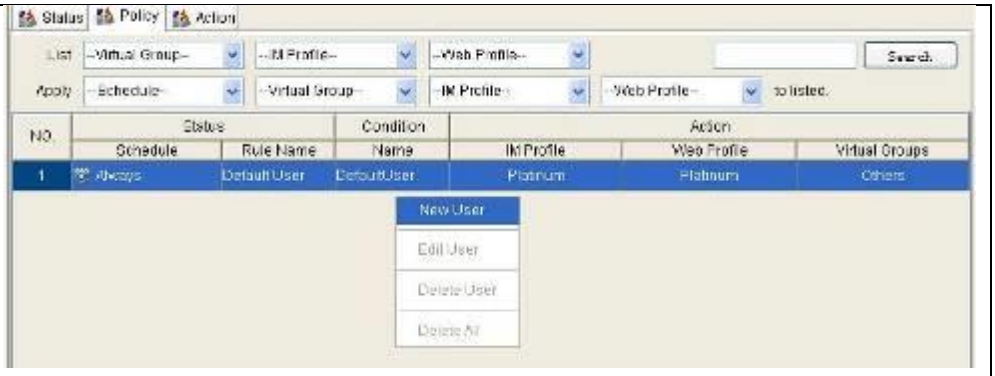


(Fig.2)

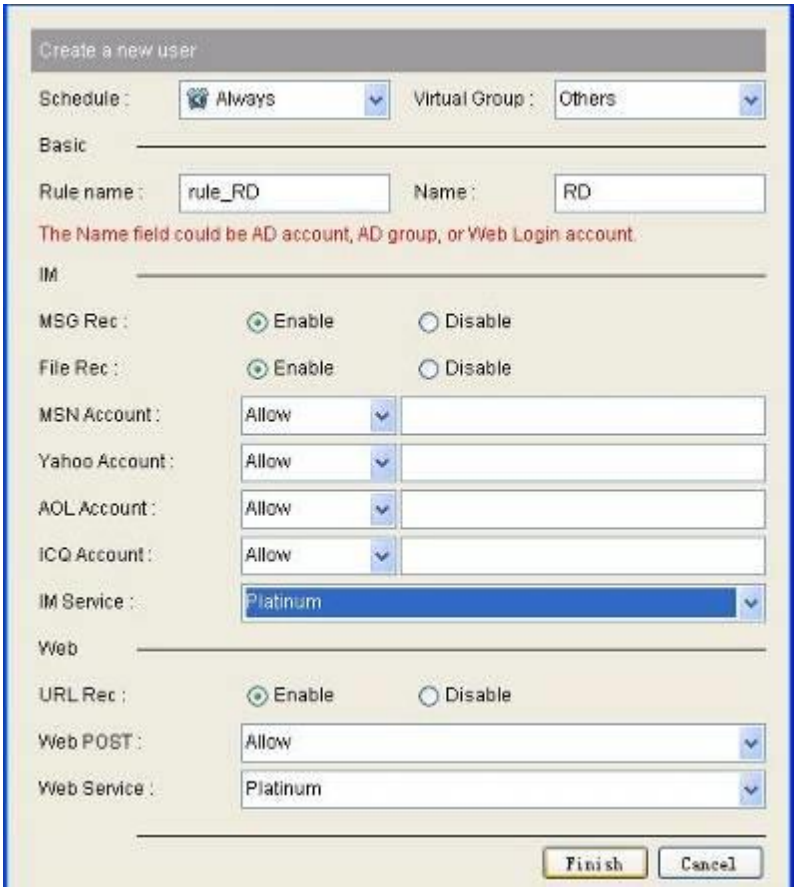
10.3.2.2 Manually assign web-login account names in content policy rules

Step 1 Add a new rule Here we want to audit the IM conversation, file transfers,	**Functions > Content Manager > Content Policy > Policy**

URL access of the RD group. First, right click on the policy area and select the New User to add a rule. Fill in the Name field with "RD" and check the Enable of the MSG Rec and the File Rec. Upload the configuration.



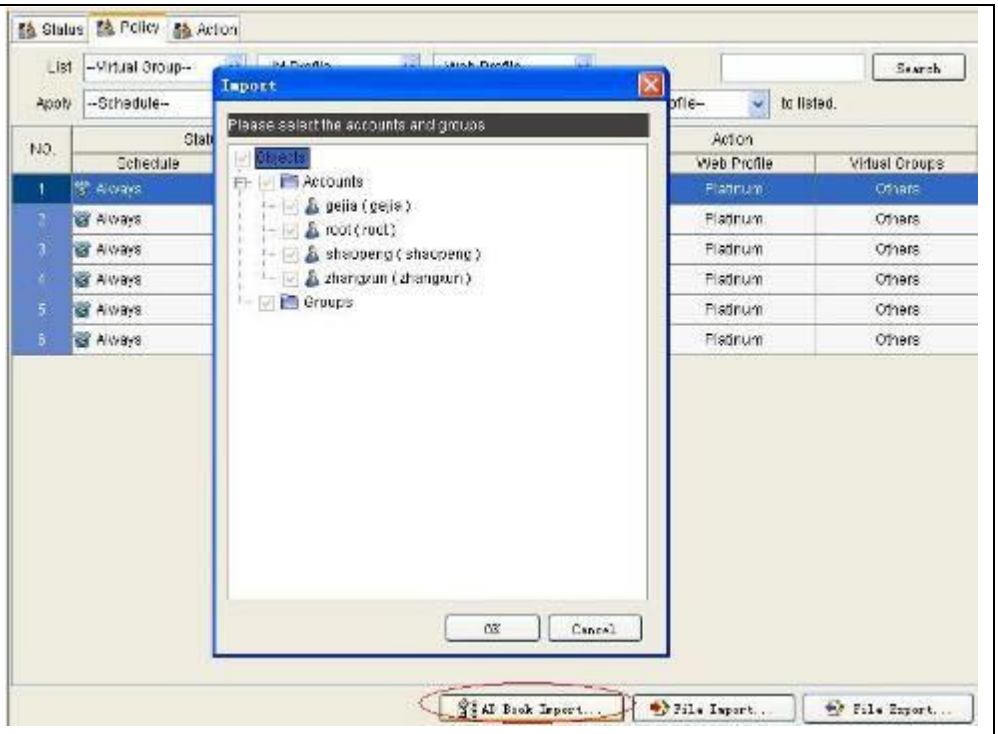
(Fig.1)

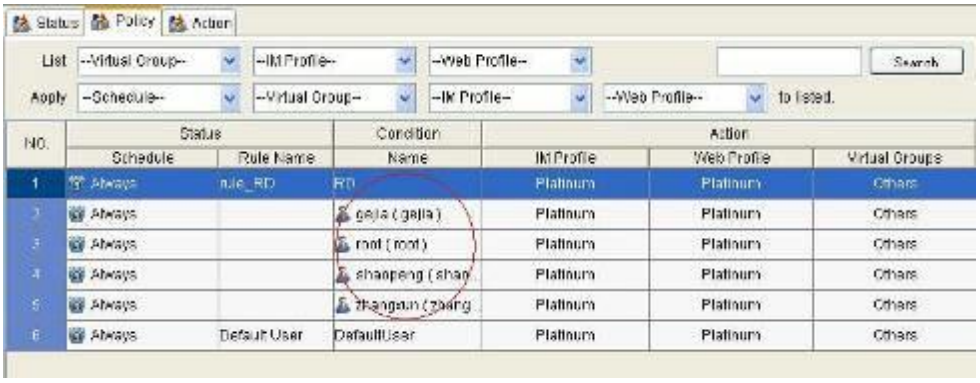


(Fig.2)

10.3.2.3 Import web login users into content policy rules

Step 1 Import web login users We can import previously added web login user account names by clicking the AD Book Import. Select those users you want to import and press OK to proceed.	**Functions > Content Manager > Content Policy > Policy**


Status
Policy
Action
List
--Virtual Group--
Apply
--Schedule--
Search
to listed.
Import
Please select the accounts and groups
Objects
Accounts
gejia (gejia)
root (root)
sheopeng (sheopeng)
zhangxun (zhangxun)
Groups
OK
Cancel
NO.
Schedule
Action
Web Profile
Virtual Groups
Always
Platinum
Others
AD Book Import...
File Import..
File Export...


Status
Policy
Action
List
--Virtual Group--
--IM Profile--
--Web Profile--
Search
Apply
--Schedule--
--Virtual Group--
--IM Profile--
--Web Profile--
to listed.
NO.
Status
Schedule
Rule Name
Condition
Name
Action
IM Profile
Web Profile
Virtual Groups
Always
rule_RD
RD
gejia (gejia)
root (root)
sheopeng (shep
zhangxun (zhang
Default User
DefaultUser
Platinum
Others

Chapter 11
Configure APP/Content with AD Single-Sign-On

This chapter introduces how AD single-sign-on gets users' identity for APP/Content policy

11.1 Scenario

1. Generate reports with IP addresses mapped to AD user/group names.
2. Configure APP/Content policy rules by matching AD user / group names.

11.2 Methodology

1.1 Map IP addresses in reports to AD user account names
- 1.1.1 Add a Domain Controller (DC) in Windows 2003 Server
- 1.1.2 Add an AD user account in a Windows 2003 Server
- 1.1.3 Use the newly added accout at Windows client PC to login to the AD Server
- 1.1.4 Execute AD Import
- 1.1.5 Install AD logon script into the AD Server
- 1.1.6 Configure device to accept AD login events
- 1.1.7 Relogin from Windows client PC and check "sys ad show" to see if the PC appears

1.2 Configure policy rules to match AD user accounts for filtering
- 1.2.1 Go to [Object Manager -> Dynamic Objects] Import all user account names from the AD server.
- 1.2.2 Assign AD user accounts / AD groups in App Policy rules
- 1.2.3 Assign AD user accounts / AD groups in content policy rules
- 1.2.4 Import all AD user accounts into content policy rules.

11.3 Steps

11.3.1 Map AD User Accounts to IP in Reports

11.3.1.1 Add a Domain Controller (DC) in Windows 2003 Server

Step 1 Add components

As an example, if the AD server is Windows 2003 Server with client PC using Windows XP Professional (Windows XP Home does not support AD):
DC Name: www-f4b3ffe209b
IP address: 192.168.18.190
Netmask: 255.255.255.0
Gateway: 192.168.18.1

DNS : 192.168.18.190 (this machine itself is to be a DNS server.

By default, DNS Server component is not installed. So we need to add the component by ourselves. Go to "Control Panel-> Add or Remove Programs", click the "Add or Remove Windows Components" , you will see the "Windows Components Wizard" as in Fig.1.

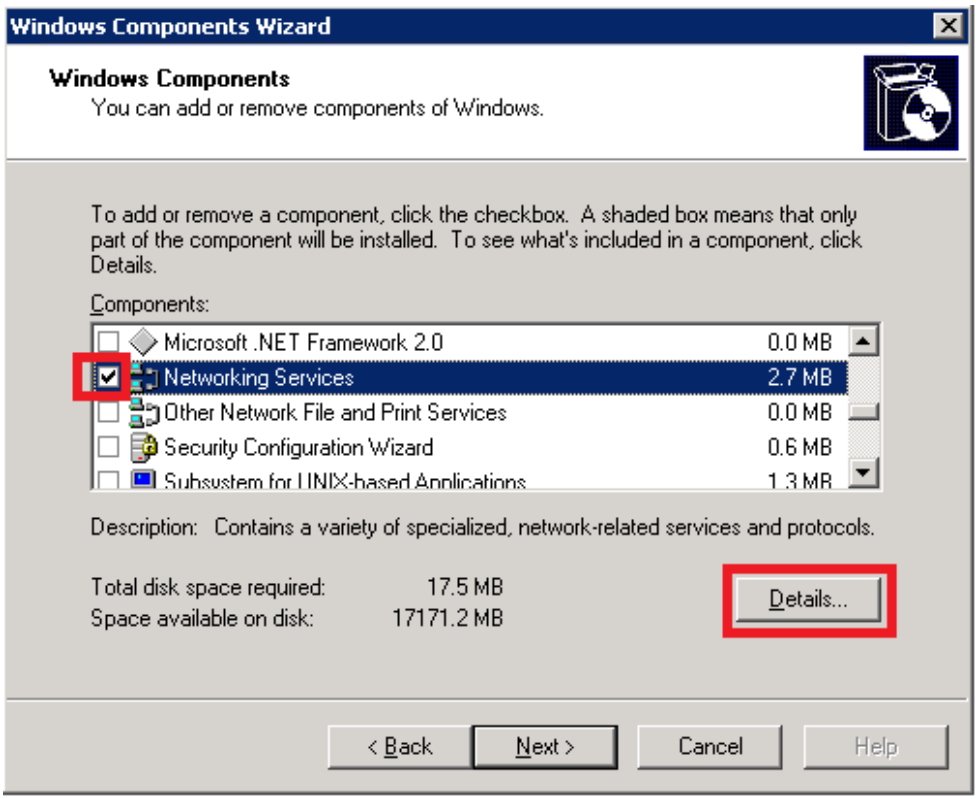


Fig.1

By default, all network services are added. Click the "Details..." to choose the componets by yourself. Check only the DNS Server and uncheck all the others as Fig.2 shows.

Finally, click the "OK" and continue to step next to finish the DNS Server installation. Please make sure that the CD of Windows Server 2003 is available. Otherwise it will prompt you with a file not found alert and require manually setup the path.

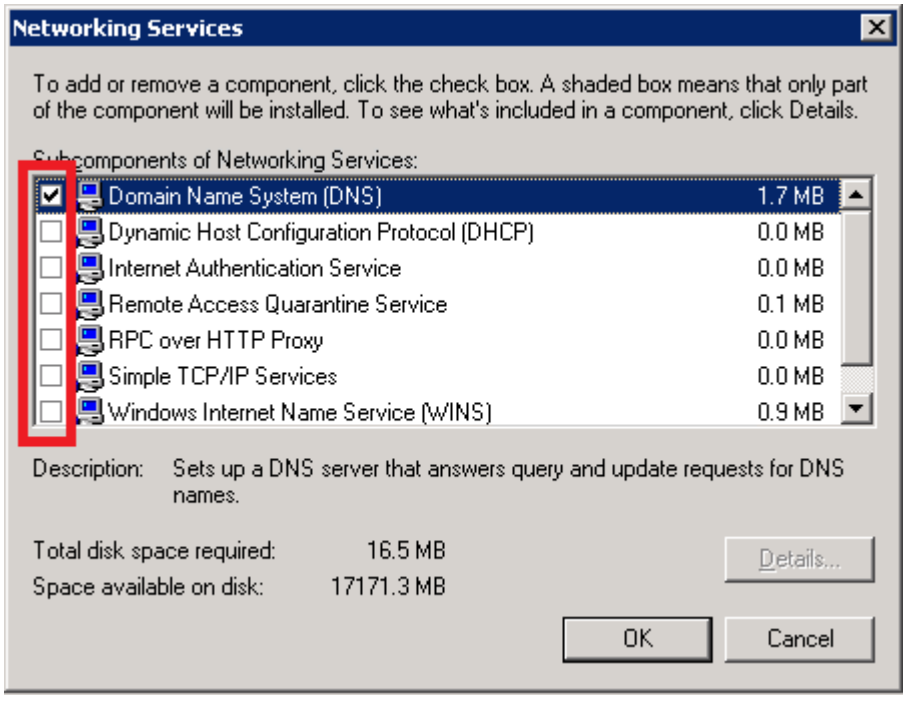


Fig.2

Step 2 Install AD

After installing DNS Server, we can start to install Active Directory. Go to "Start->Run" to enter "dcpromo" you will see the "Active Directory Installation Guide". Click the Next button in Fig.1.
There will be a compatibility requirement that PCs' versions must be newer than Windows 95 and NT 4 SP3 cannot logon to the DC of Windows Server 2003. We suggest to at least use Windows 2000 or newer versions of Windows to be the AD client machines.

Since it is the first domain controller, we choose the first option "DC for a new domain". Click the Next button to proceed (Fig.2).

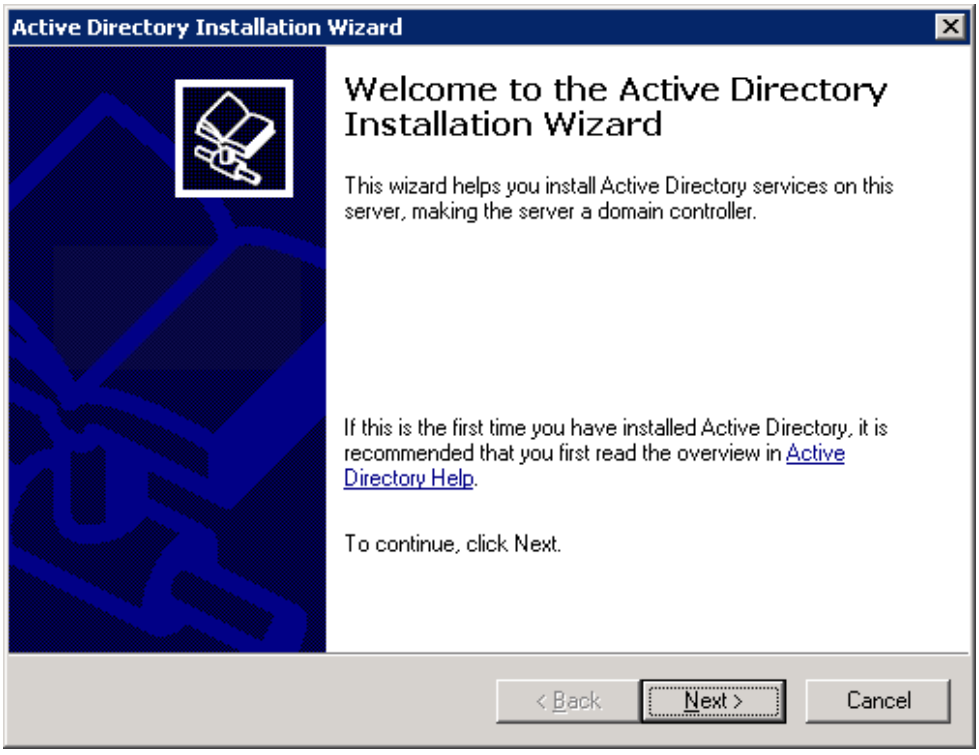


Fig.1

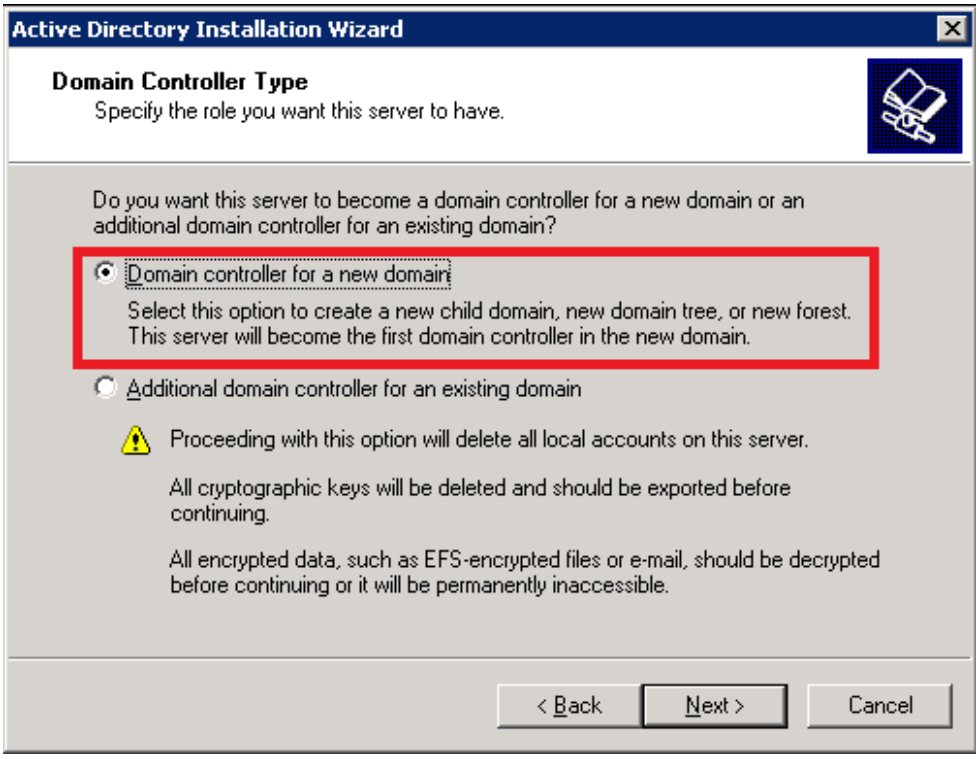


Fig.2

Since it is a new domain in a new forest, we choose the first option as shown in Fig.3.

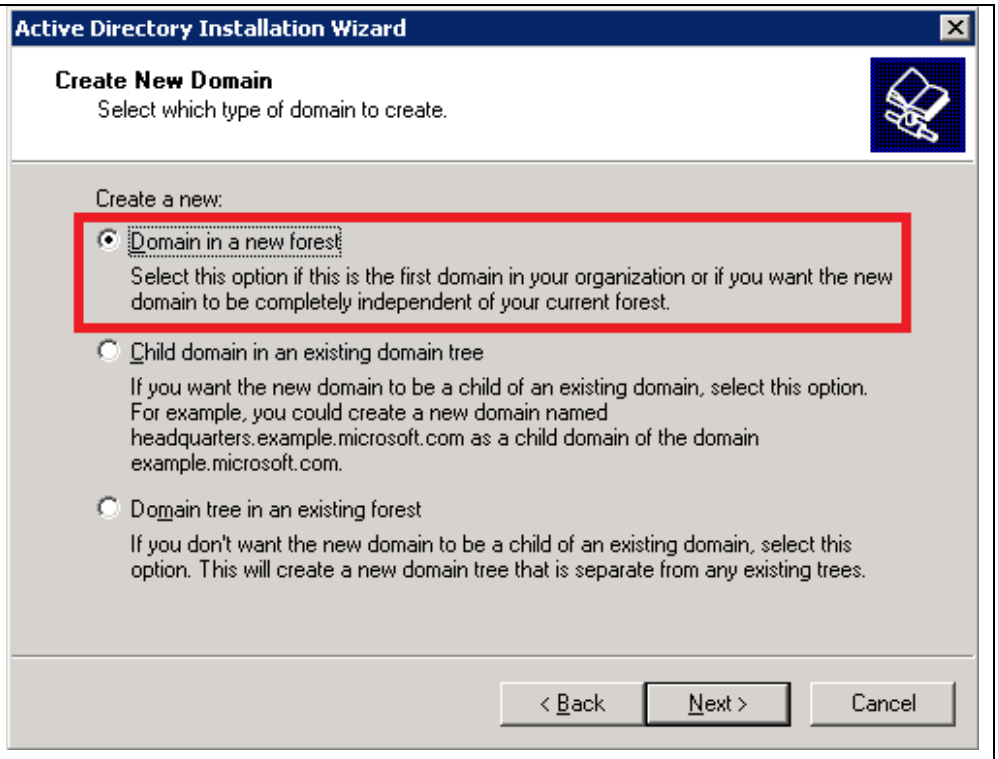


Fig.3

Next, we need to assign a domain. For example, we assign "test.com" as our domain name (Fig.4).

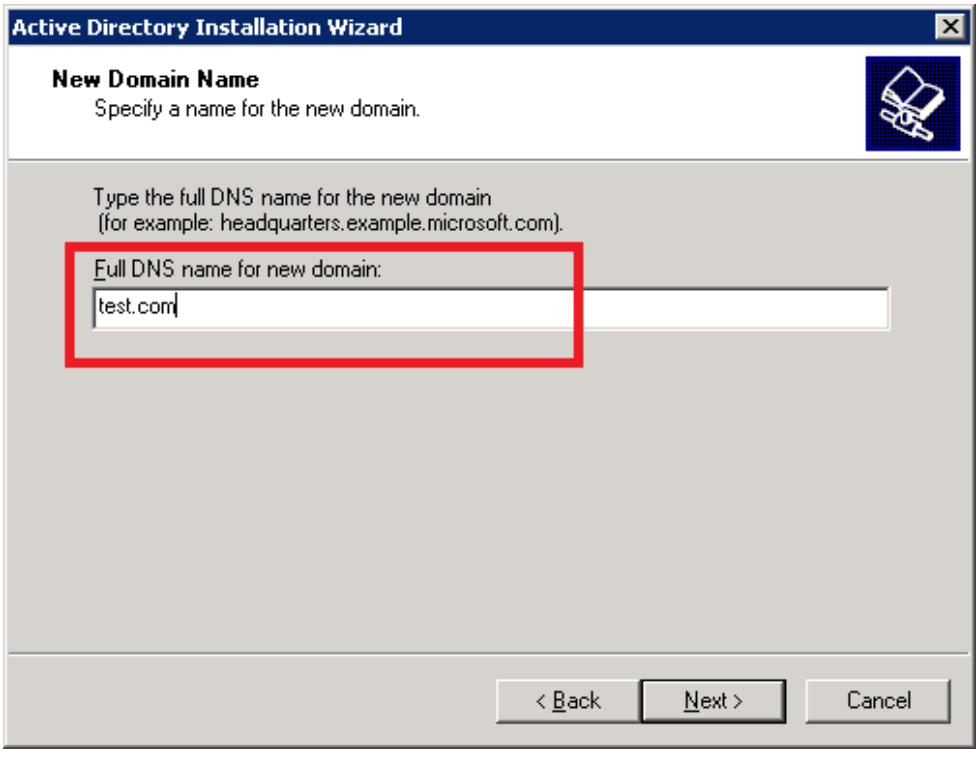


Fig.4

Then enter your NetBIOS name, for example, by default it gives a "TEST" as shown in Fig.5. Please be noted that the name should never conflict with PC clients in the same domain. Namely, there should never be a PC client named "test".

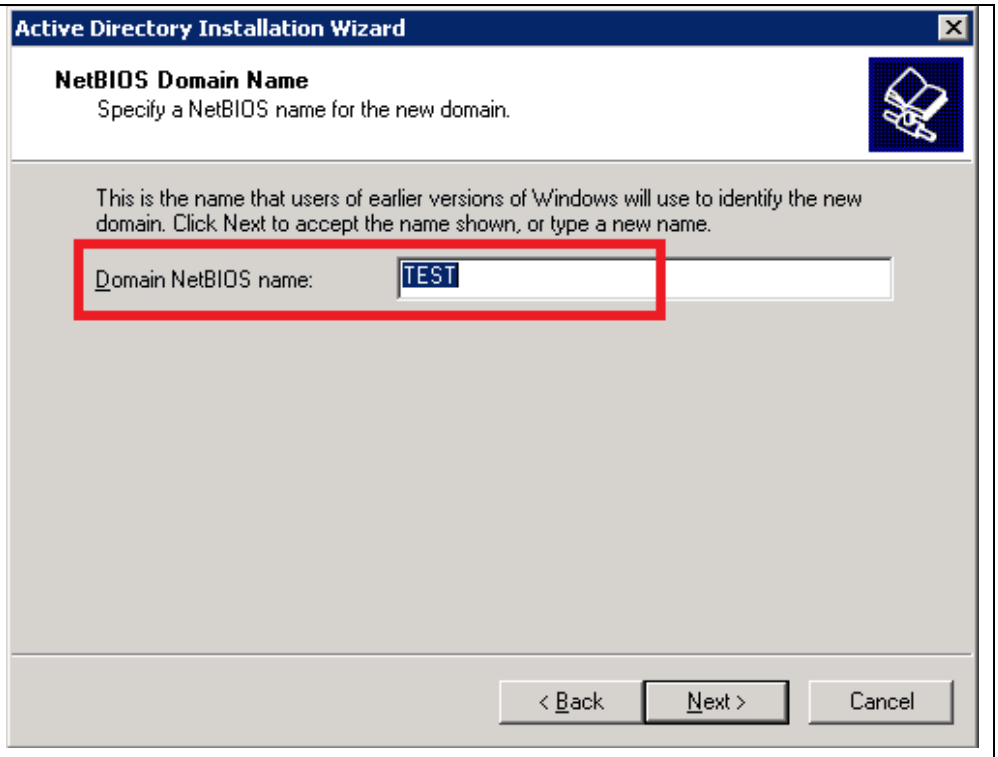


Fig.5

Next, we need to assign the path to store the AD database and the event logs. If the space in drive C is sufficient enough, keep the default setting as shown in Fig.6.

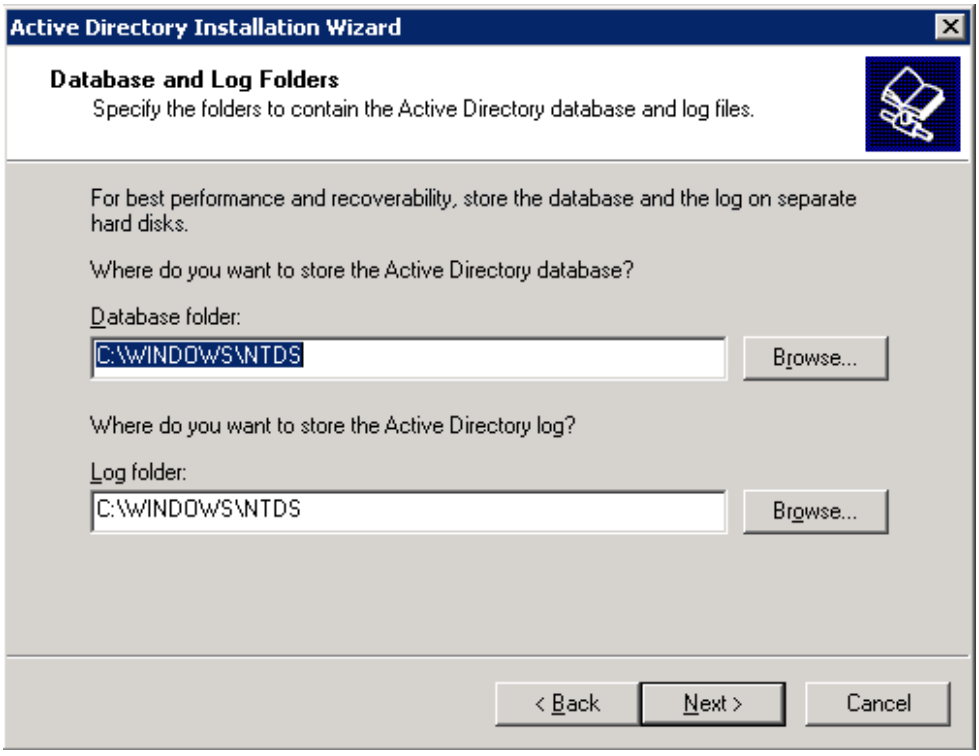


Fig.6

Next, we need to setup the Shared System Volume. We suggest to leave the default path as shown in Fig.7.

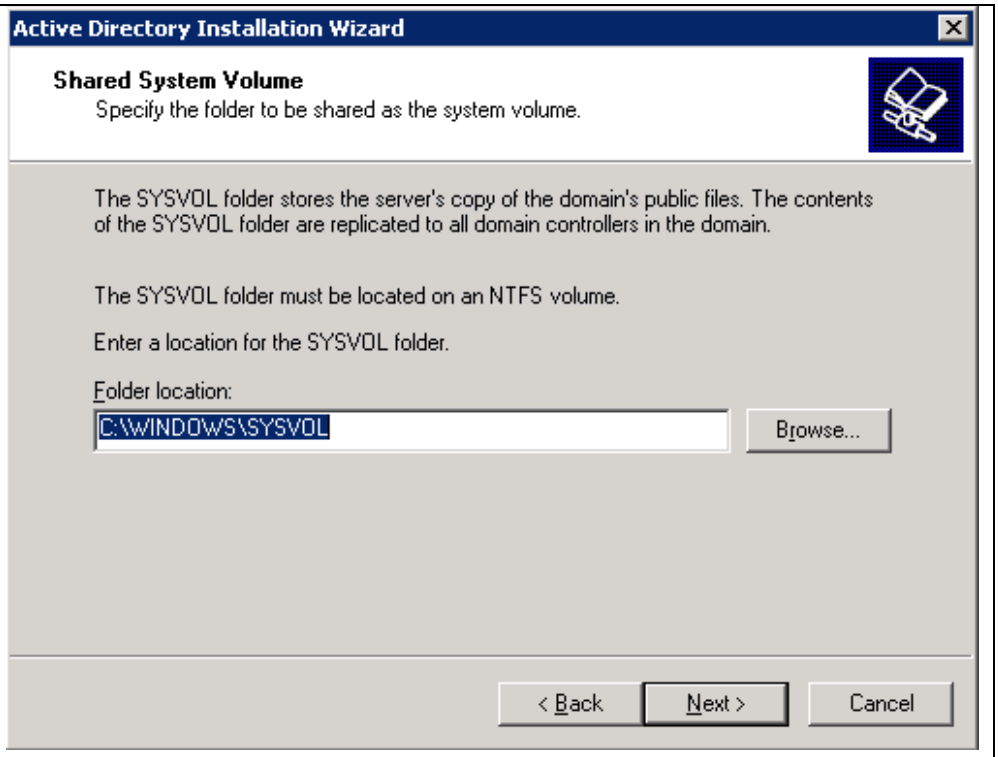


Fig.7

Noted that the first installation always encounters the DNS failed problem. Although we have installed the DNS server, but we have not configured it so there is no DNS server to respond. Here we are to configure the DNS server and make this server as the first DNS server (Fig.8).

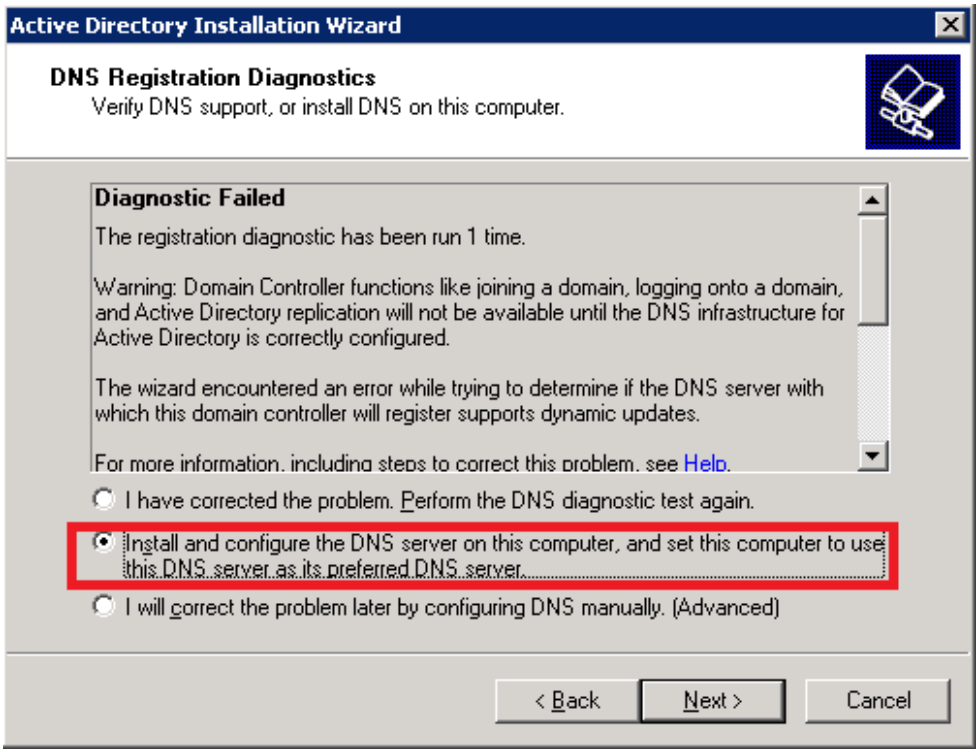


Fig.8

Next, we choose default permissions for user and group objects (Fig.9). We choose the second option that only compatible with Windows 2000 or Windows Server 2003 if the environment has no operating systems older than Windows 2000."

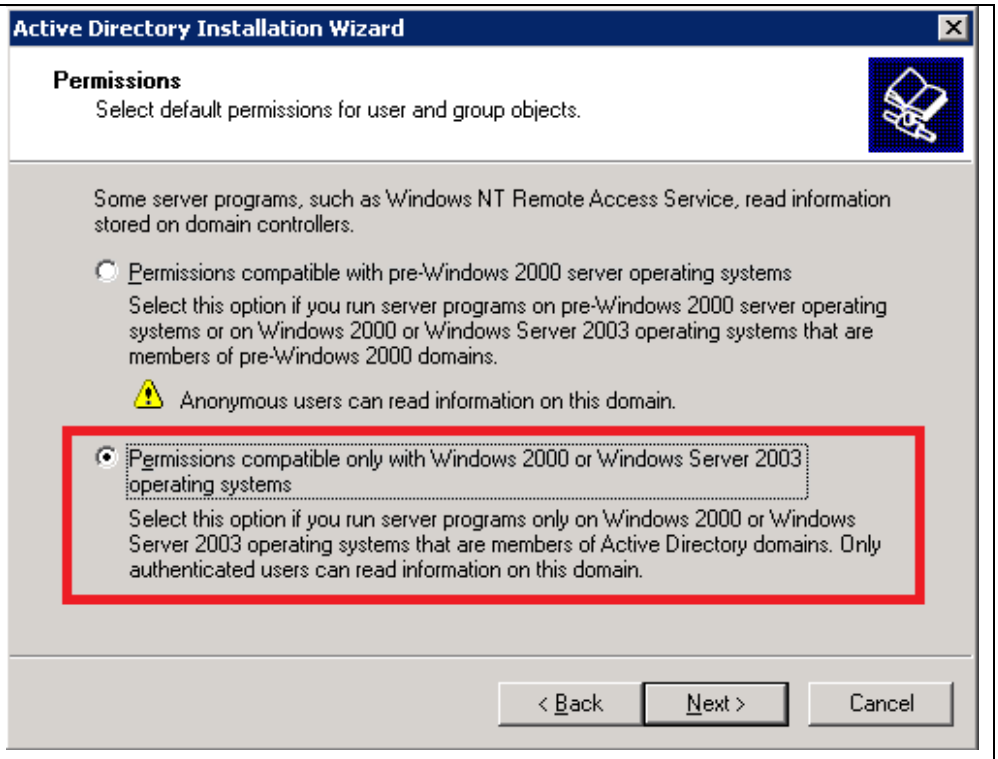


Fig.9

Next, we have to setup the restore password. Please remember this password very carefully.

Fig.10 is to confirm all the above settings.

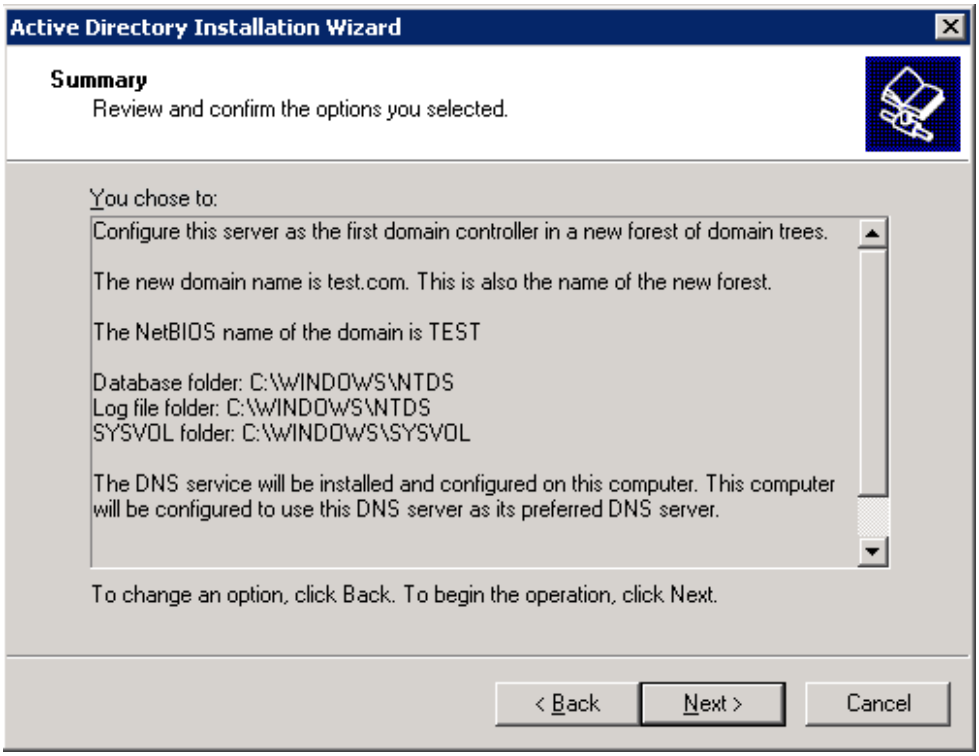


Fig.10

Once you click the Next button, the AD server is being installed with the software as Fig.11 shows. A few minutes later, the installation process will complete. Sometimes it requires more time, especially when it configures the DNS service.

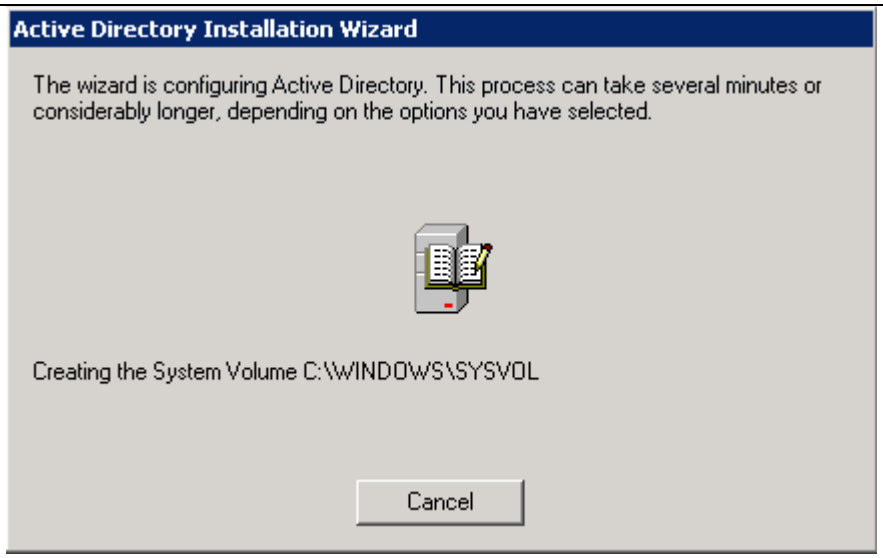


Fig.11

The software is finally installed as Fig.12 shows.

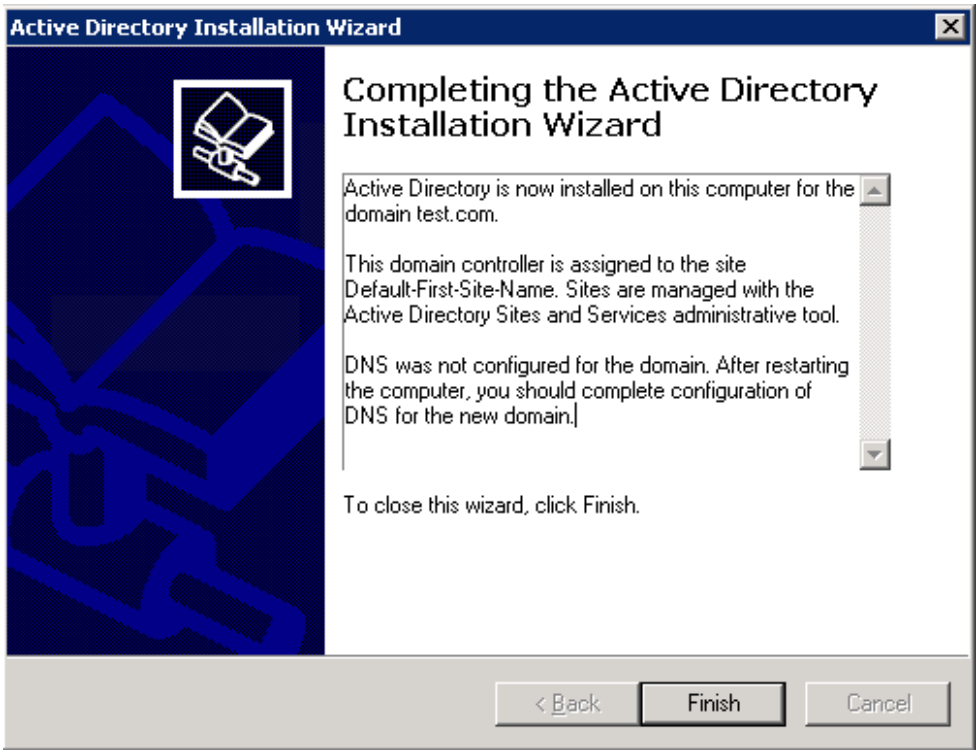


Fig.12

After you click the "Finish" button, it will prompt you to reboot immediately. Click the "Restart Now" to reboot the system.

Fig.13

After the reboot, we will check what are the differences. First of all, we will find that the speed for booting or shutdown the system becomes slower. And we can see that the login user interface contains a new field "Log on to". Choose the "TEST" domain to login, then we will be login to the TEST AD domain.

Fig.14

After we have successfully logged into the system, we can check the "My Computer -> Properties". Click the "Computer Name" tab (Fig.15), you will be seeing that the domain is "test.com". In this way, we have make a normal Windows 2003 Server become a Domain Controller (DC).

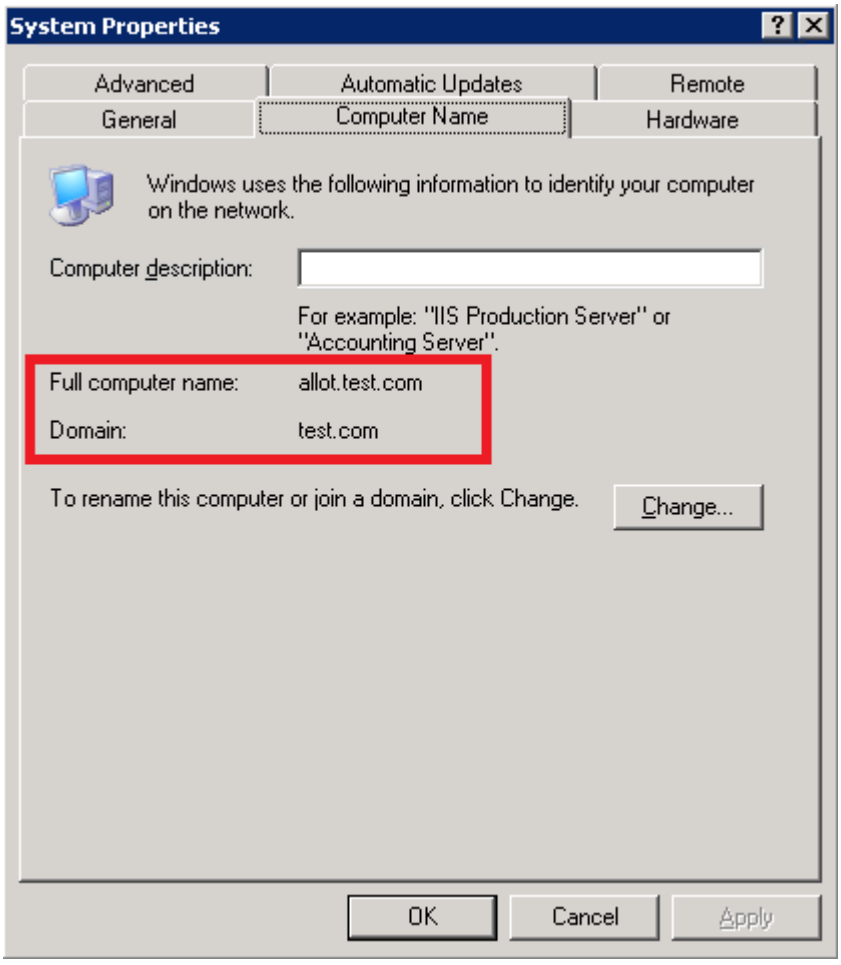


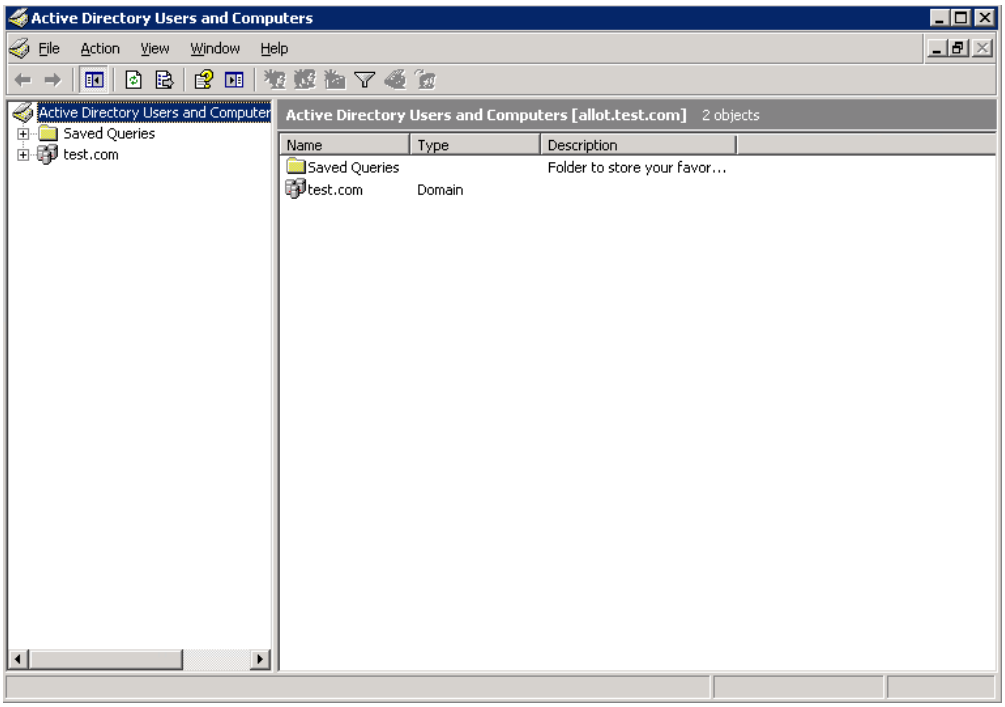
Fig.15

11.3.1.2 新增 AD 用戶

Step 1 Add an AD account at the AD Server

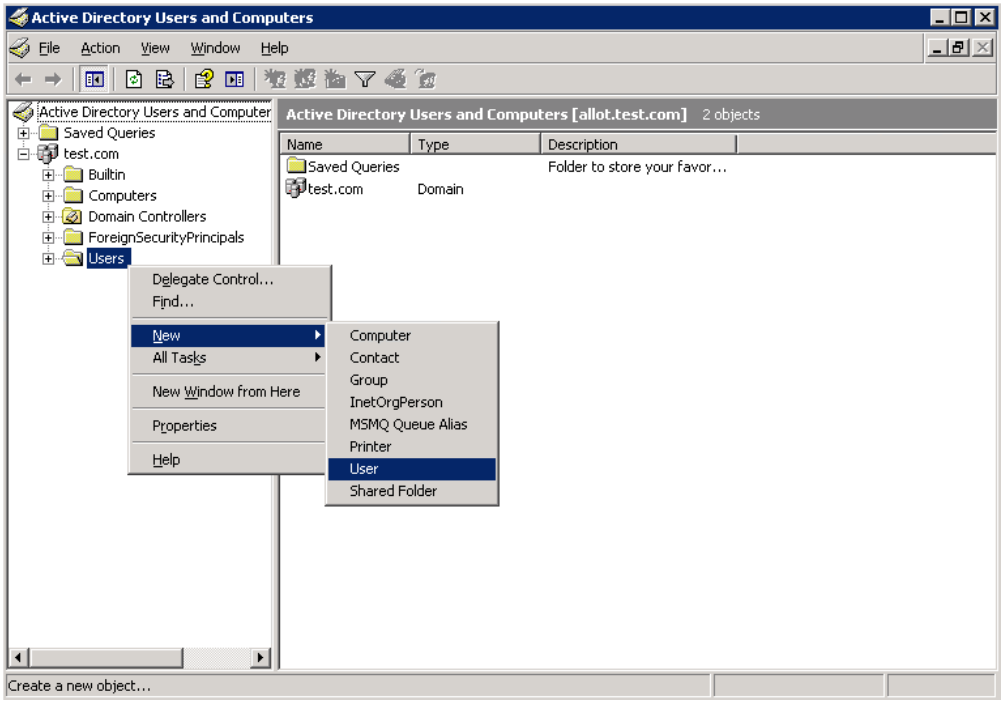
For security reasons, it is not suggested to use administrator so oftenly. So we create a new account first:

Login to the DC and run the program "dsa.msc". There will be a "AD Users and Computers" management console as Fig.1 shows. We use this console to create a new account.



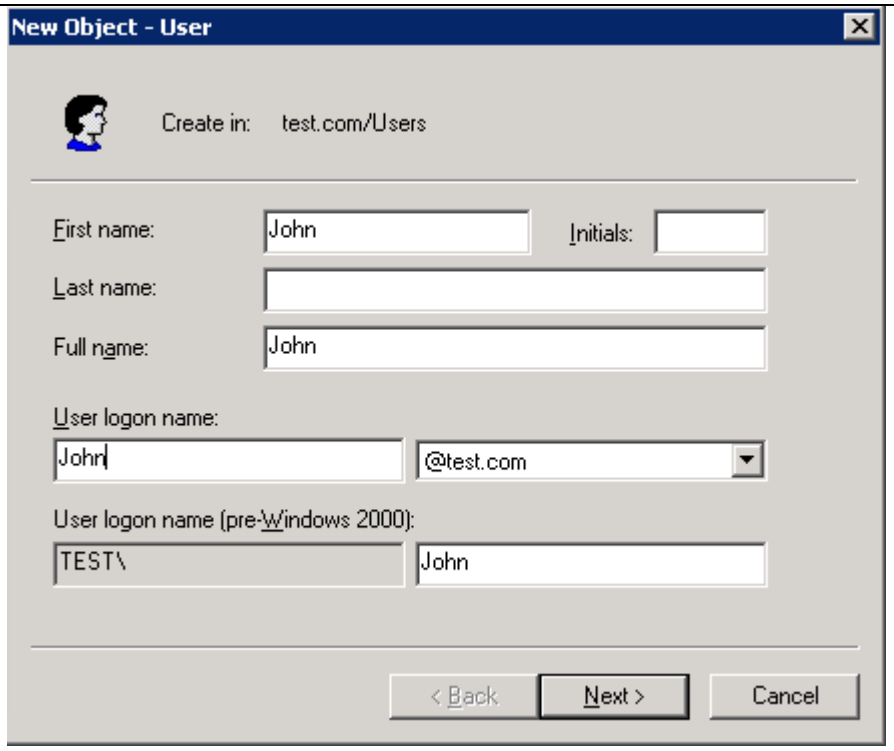
(Fig.1)

First, expand the "test.com" and right click on the "Users". Choose "Create->User" as Fig.2 shows.

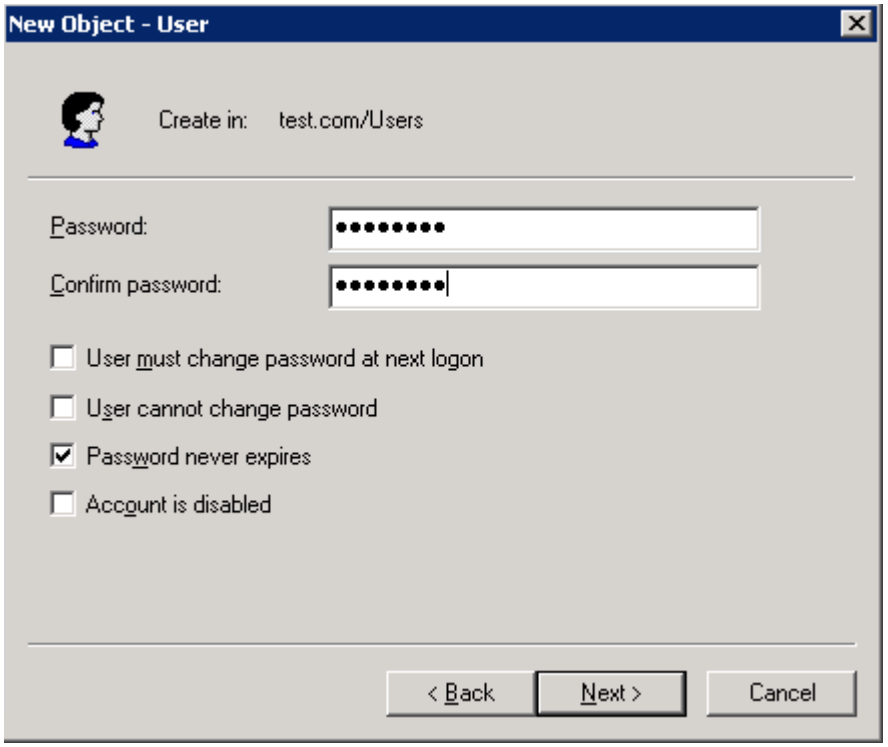


(Fig.2)

There will be a new wizard. We create a new name called "John" and set the password as "Never expired" as shown in Fig.3 and Fig.4. Click the Next button to proceed to finish the creation of the user.



(Fig.3)



(Fig.4)

Step 2 Delegate Control

Right click on the "test.com" and select the "Delegate control" as Fig.1 shows. There will be a "Delegation of Control Wizard" running as Fig.2 shows.

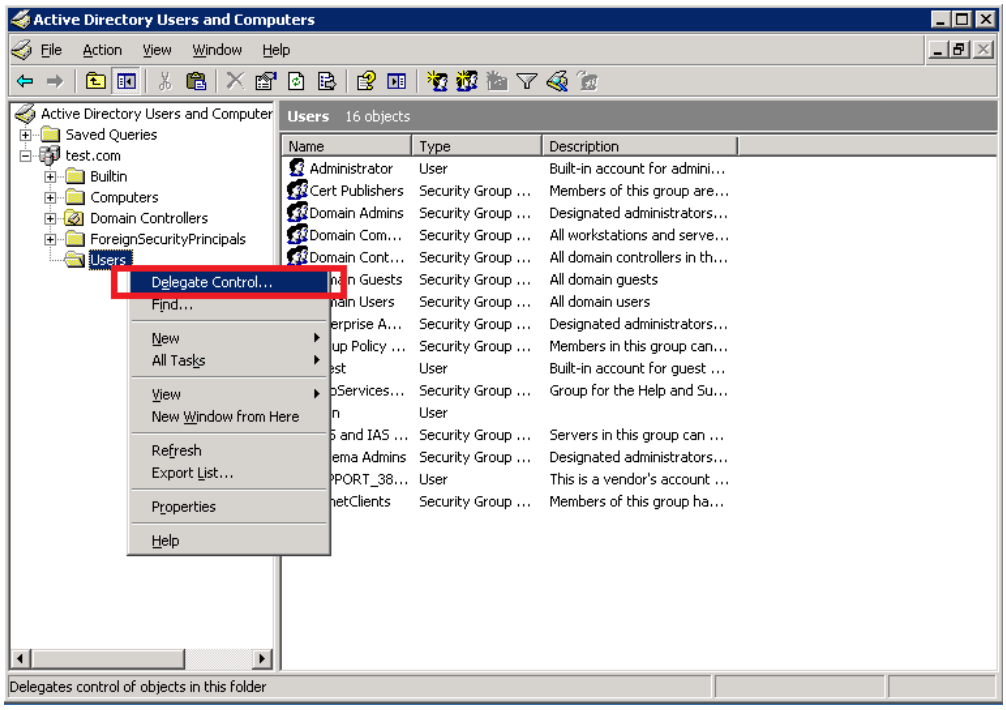


Fig.1

Fig.2

Click the "Add" button to add the previously created account "John" as Fig.3 and Fig.4 show.

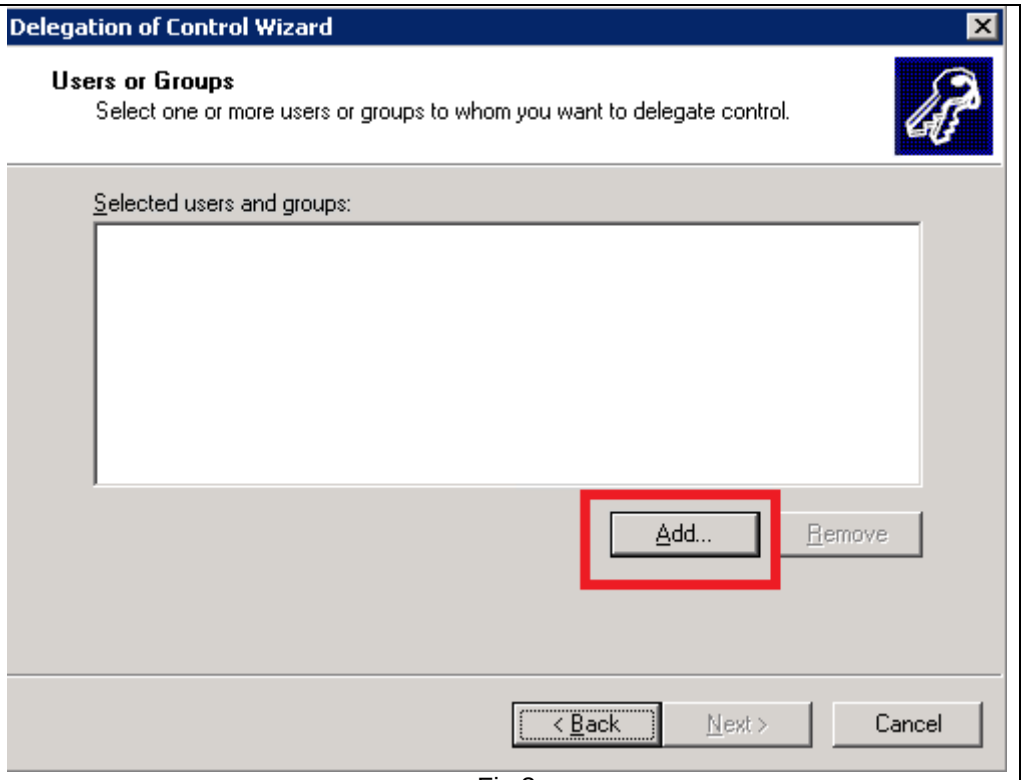


Fig.3

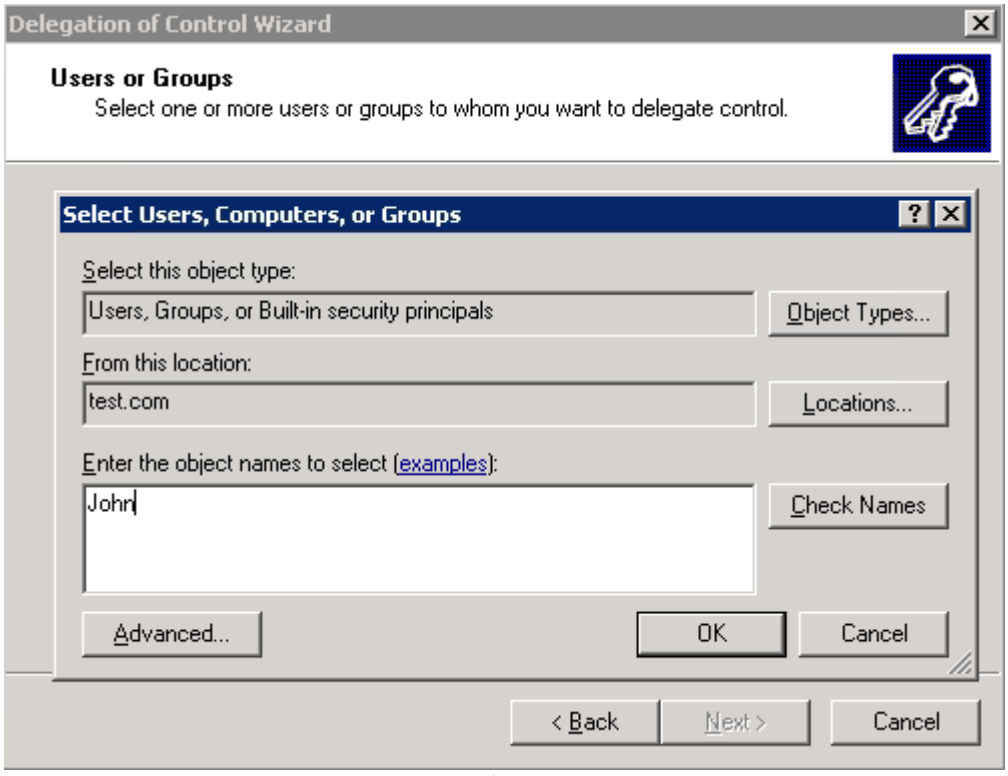


Fig.4

Here John is added into the list for delegation of control.

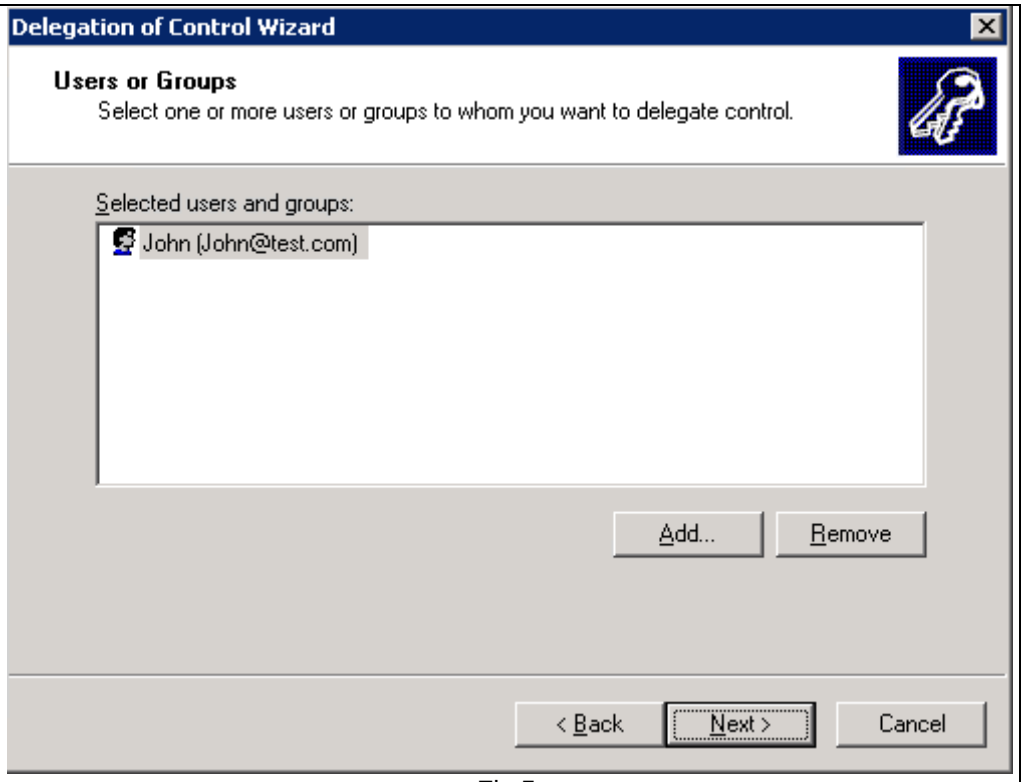


Fig.5

Next, we choose to allow John to have the permission to "Create, delete, and manage inetOrgPerson accounts". Click the Next button to proceed as Fig.6 shows.

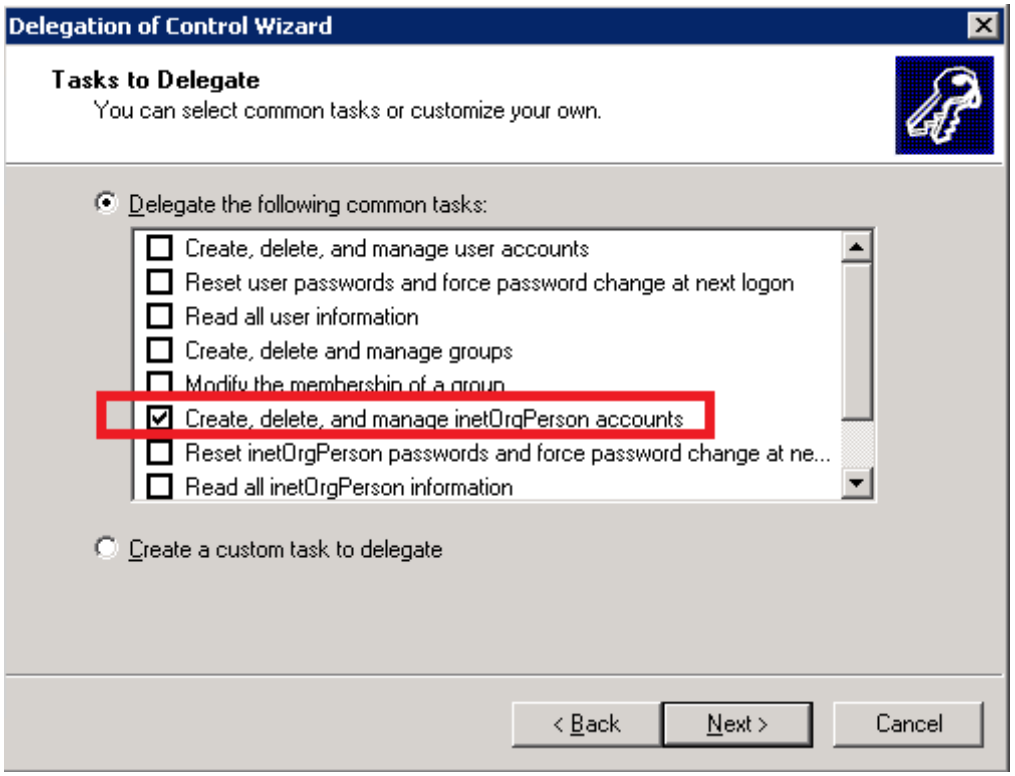


Fig.6

Click the "Finish" button to confirm that John is authorized to control the computers to be added / removed to the domain.

Fig.7

11.3.1.3 Make Windows 2000/XP/2003/Vista/Windows7 PCs Login with newly added AD accounts to the AD domain

Step 1 Setup network properties

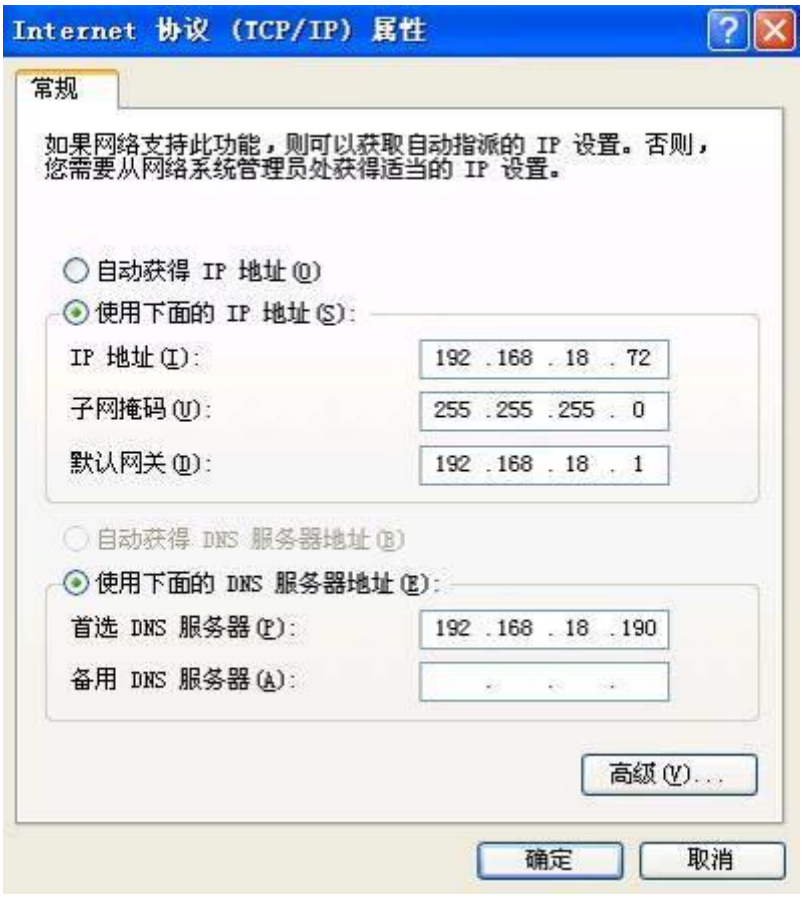
We use Windows XP as an example to show how to add itself into the new AD domain. Other Windows systems are alike. Please be noted that usually only Professional / Server version of Windows have the feature. Home versions cannot join the AD domain. We start configuring this by setting up the network properties of the Windows XP as Fig. shows:

Computer Name: : MyName

IP:192.168.18.72

Netmask: 255.255.225.0

DNS Server: 192.168.18.190



(圖 1)

Step 2Switch to domain users

Right click on the "My Computer" and select "Properties", fill in the computer name field.

At the

在這裡把“隸屬于”改成域，並輸入:“test”，並點確定（圖 2），這是會出現如下畫面（圖 3）:

輸入剛剛在域控上有許可權的帳號，一般帳號是“Administrator”，密碼就填入它的密碼，點確定:

出現上述畫面就表示成功加入了，然後點確定（圖 4），點重啟就算 OK 了。

（圖 2）

（圖 3）

（圖 4）

Step 3 Login to AD domain

As shown in Fig.1, you can choose to login to the PC itself or to login to the domain “TEST”. After logging in, right click on the "My Computer" and select "Properties". Click the "Computer Name" to verify if the domain is at the "test.com".

(圖 1)

(圖 2)

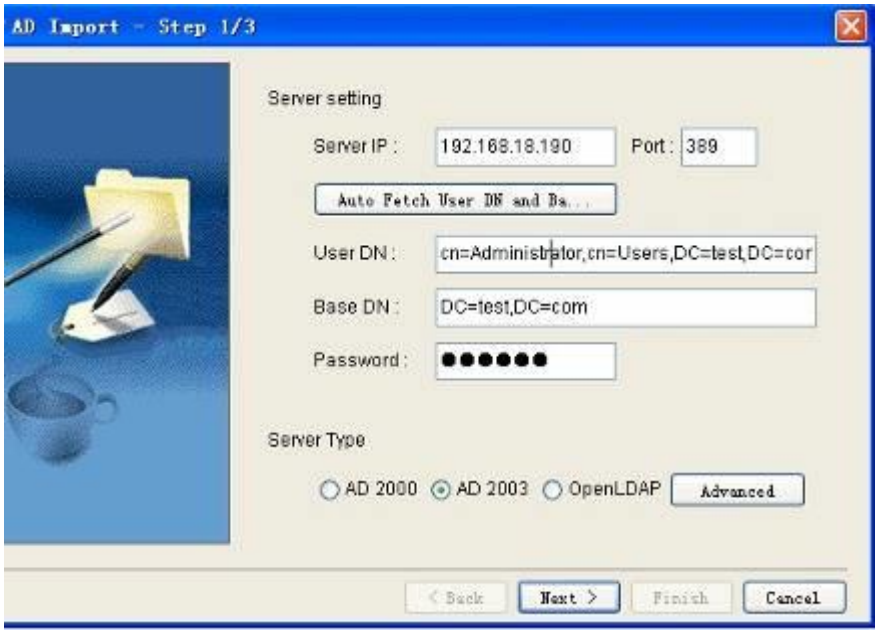
11.3.1.4 Setup AD Import at Management Server

Step 1 Setup AD Import…

Information: Windows 2003 Server IP: 192.168.18.190; Mgt Server IP: 192.168.18.45; Mgt Server OS: Windows XP Professional; Device IP: 192.168.18.92; Netmask: 255.255.225.0

Go to Object Manager -> Dynamic -> Dynamic Objects and click te AD import button.

Fill in the AD server's IP and port, then click the "Auto Fetch User DN and Base DN". You will find that the following field are automatically filled up with parameters. Enter the password for the administrator of the AD server and click the Next button.



Step 2 Select Import options

As Fig.1 shows, it has found 31 groups and 10 users. Now the system will prompt to ask for import options. The first is to delete all existing objects and then import. The second is to preserve existing objects and replace it if duplicated. The third is to preserve existing objects without importing any objects. Select one of the options and click the Next button.

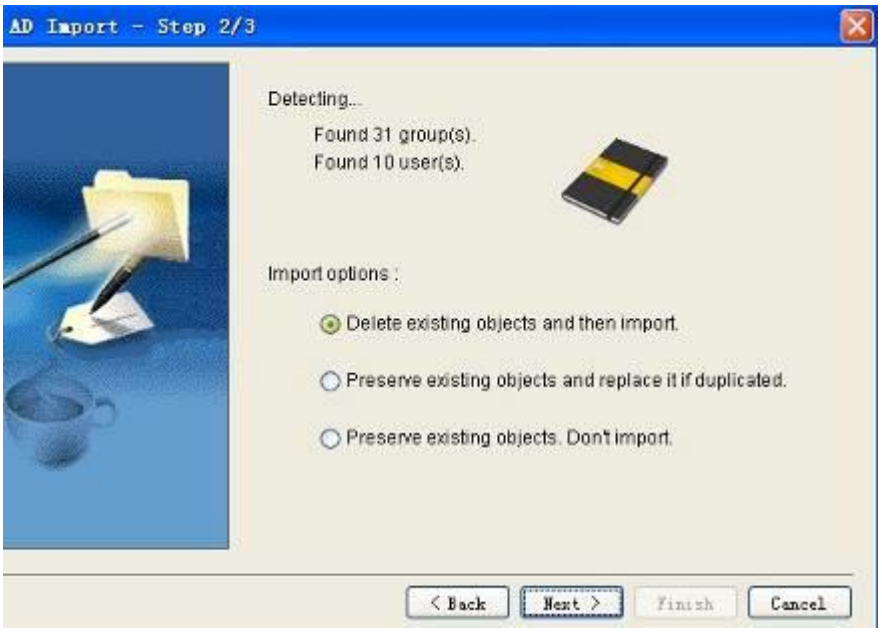


Fig.1

As Fig.2 depicts, the system has shown the users and the groups from the AD server.

Click the "Download login.vbs and adclient.exe" to download the needed files to your disk. Please copy these files to the AD server for later use.

Click the "Finish" to finsifh the AD import. Now you can see many users and groups in the dynamic objects as shown in Fig.3.

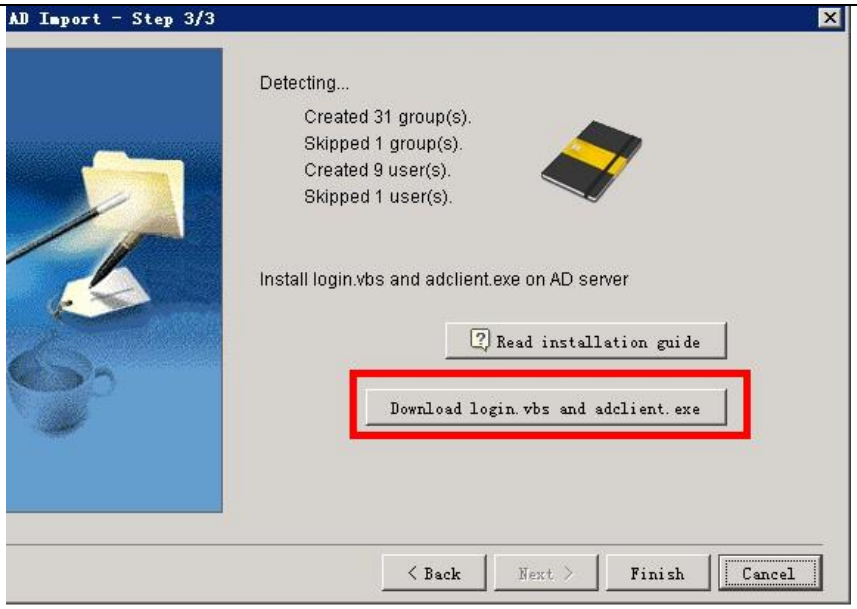


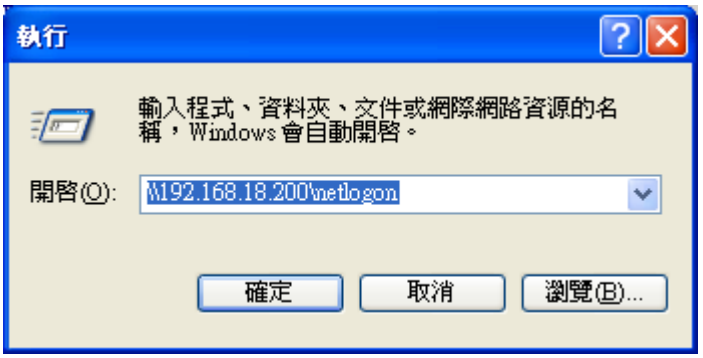
Fig.2

Fig.3

11.3.1.5 Install the login script to the AD server

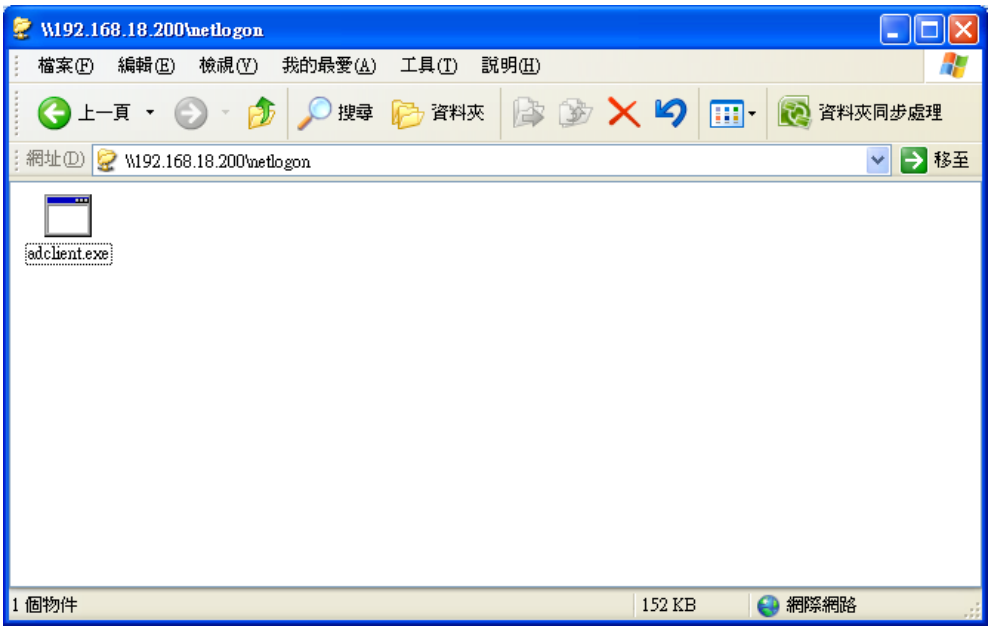
Step 1 Download files for AD server

Suppose your AD server's IP address is 192.168.18.200, with login accouting using AD's administrator, you will have the permission to open the network directory \\192.168.18.200\netlogon\



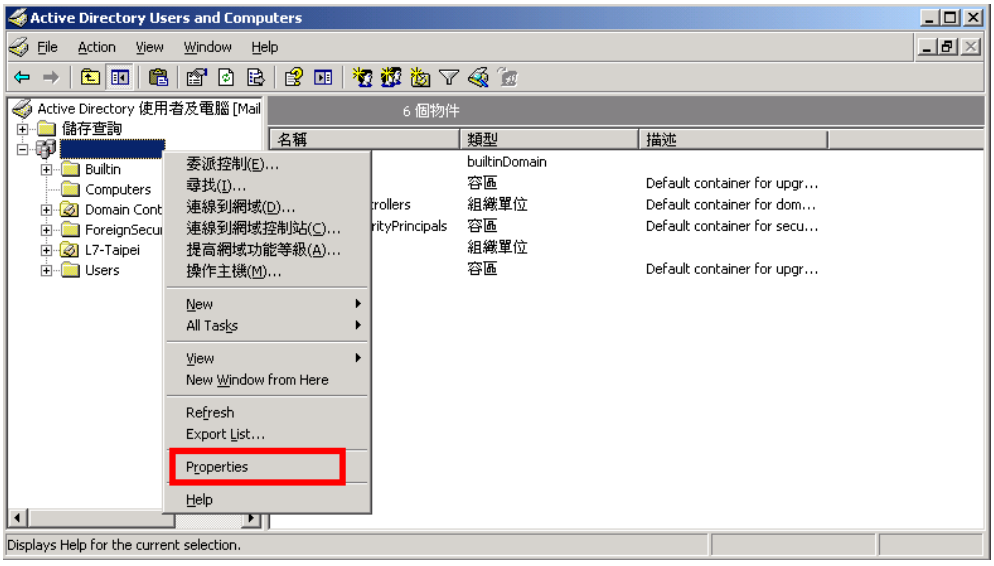
Step 2 Copy adclient.exe to the network directory

Copy and paste the adclient.exe to the network directory. Please be noted that you must use AD's administrator to login to have this permission to copy the file into that directory.



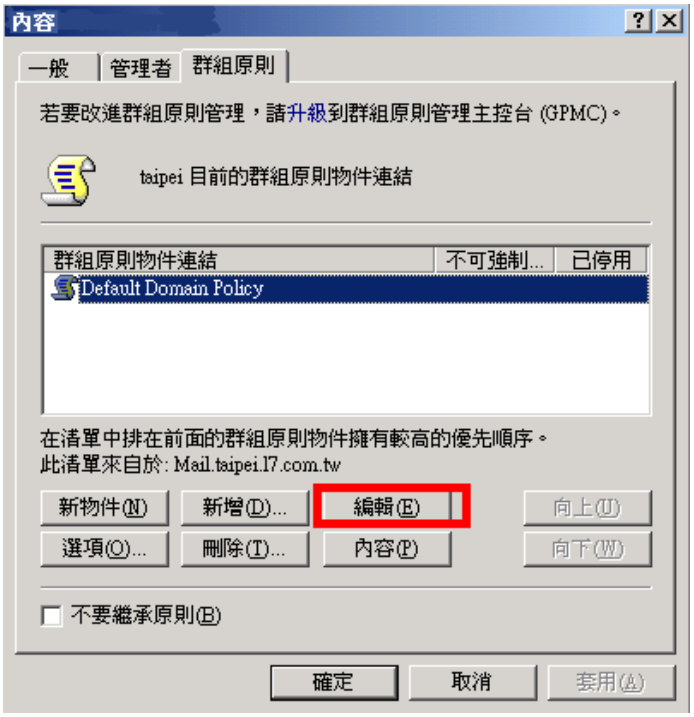
Step 3 Configure AD login Group Policy

At the AD server, please run the "dsa.msc" program. The system will launch the "Active Directory Users and Computers". Right click on your domain (eg. test.com) and click the "Properties".



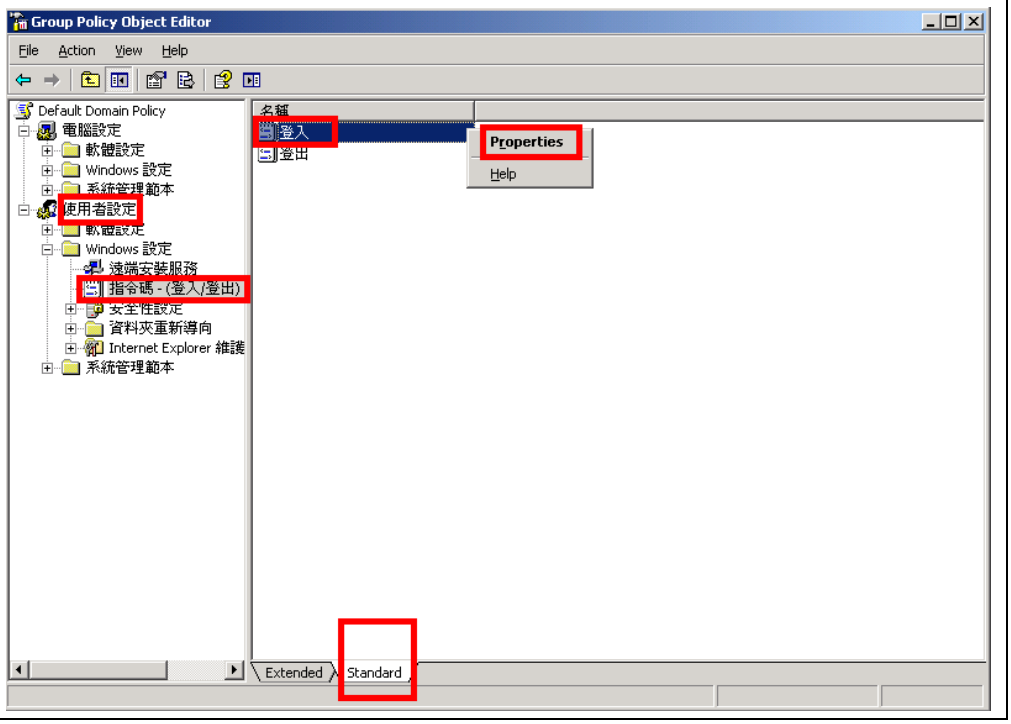
Step 4 Edit group policy

In the Properties page, select the "Group Policy" tab and click the "Default Domain Policy". Then click the "Edit" button to edit the default domain policy.



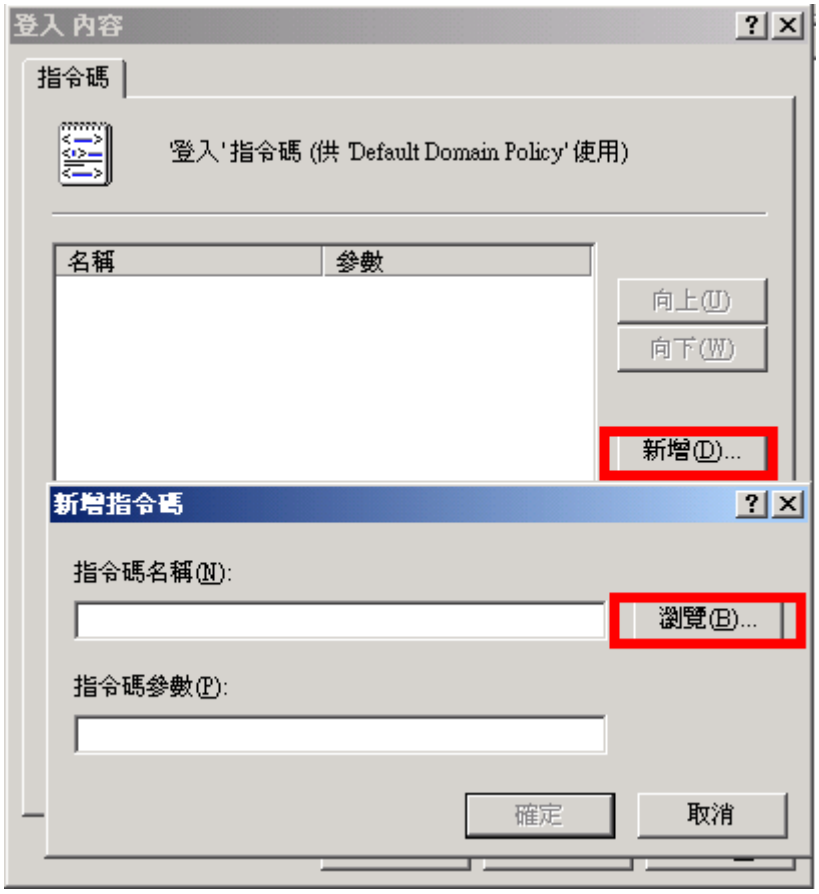
Step 5 Assign login script (I)

Use the **Group Policy Object Editor** to select [Users -> Login/Logout script]. Right click on the "Login" and select the "Properties".



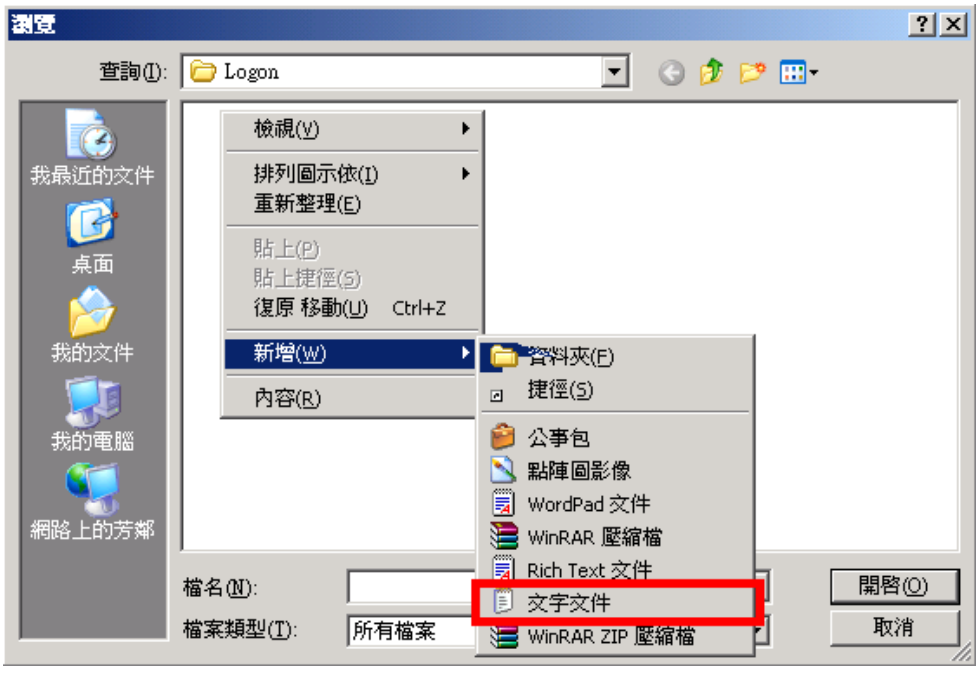
Step 6 Assign login script (II)

Choose "Add" and then click the "Browse" button.



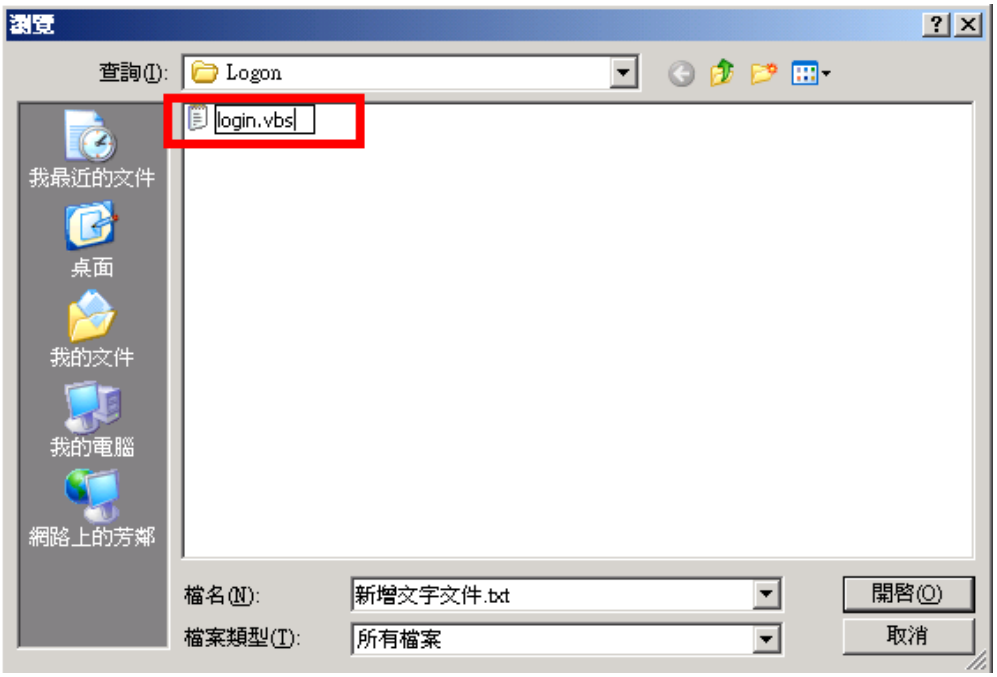
Step 7 Assign login script (III)

Right click on the blank area and select the "New->Text file".



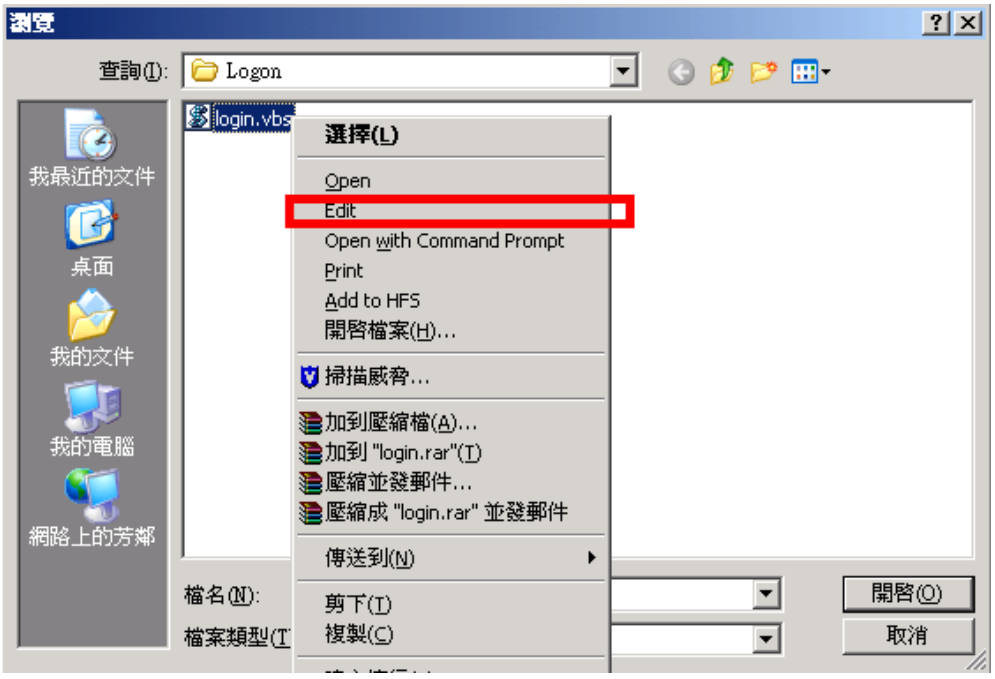
Step 8 Assign login script (IV)

Change the file name as login.vbs



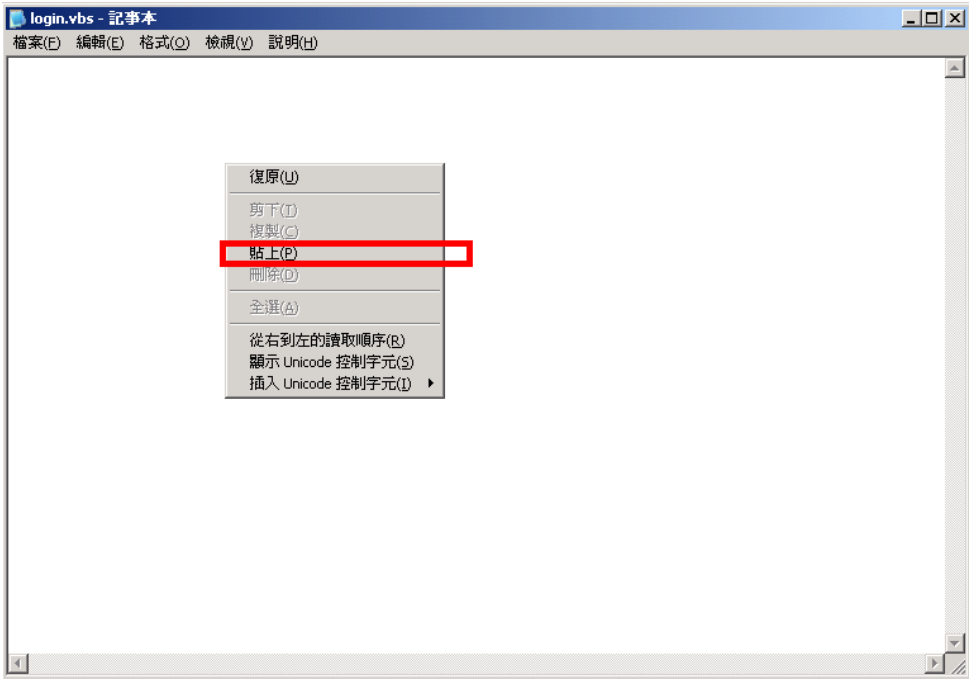
Step 9 Edit login script

Right click on the login.vbs and select Edit to edit the content of the file.



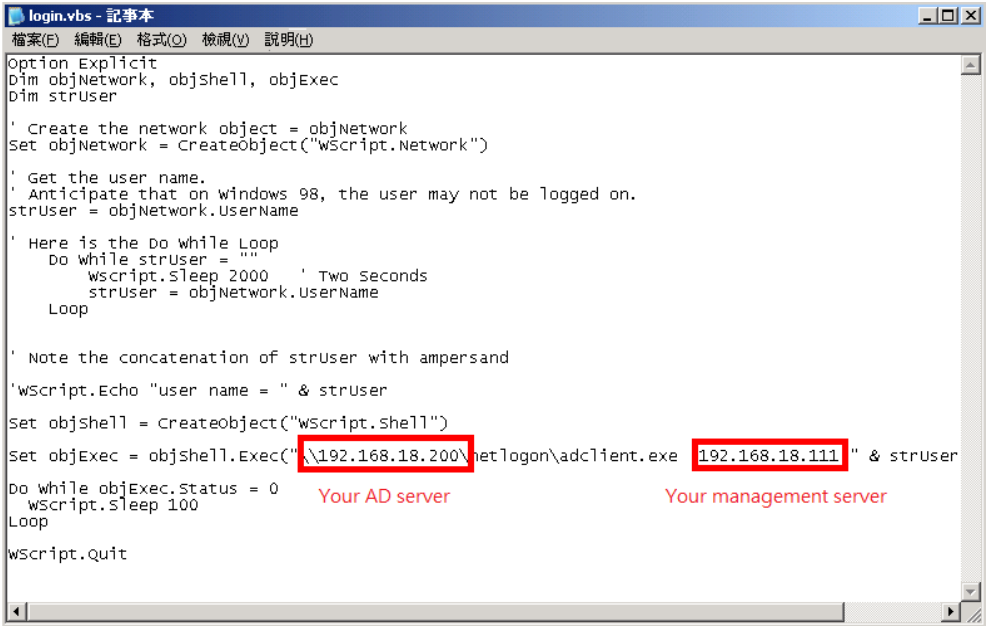
Step 10 Paste the script to the file

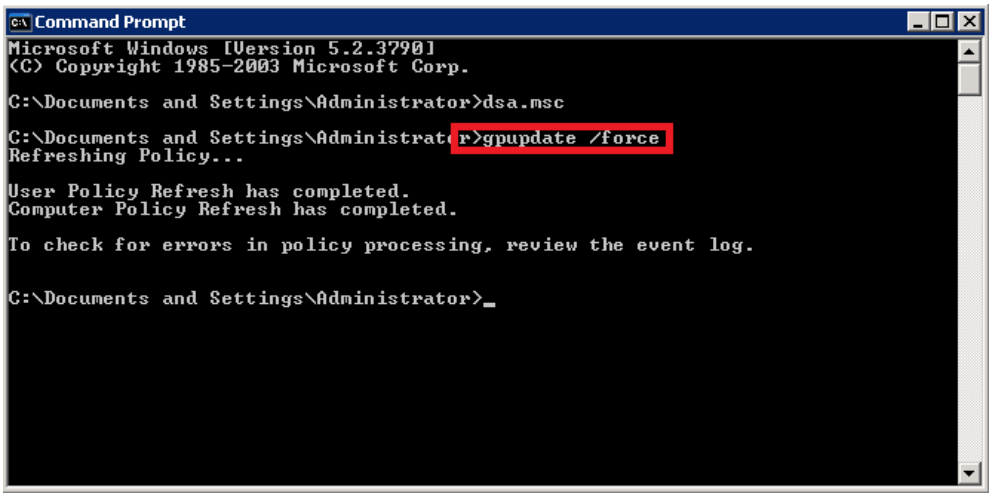
Right click on the "Paste" to paste the script to the file.



Step 11 Confirm the scrip

Confirm that the script content should be filled with correct AD server's IP and correct management server's IP. If they are all correct, please save the file.



Step 12 Refresh policy to make it effective right away After saving the login.vbs, enter the command: "GPUPDATE /FORCE" in the DOS window. If you are using Windows 7, please be sure that the DOS window must be run with administrator. You should right click on the DOS icon and select "Run with administrator".	

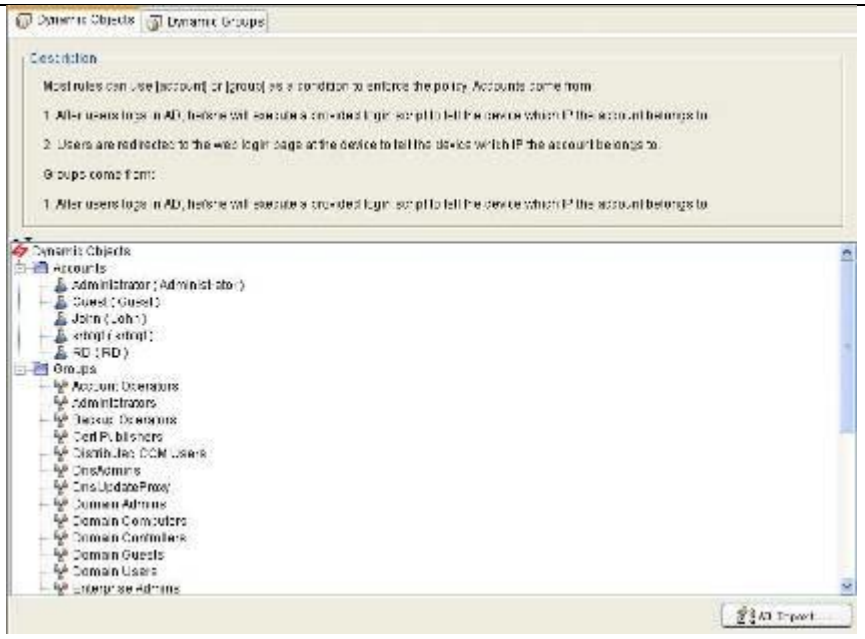
11.3.1.6 Relogin the AD User and Check with "sys ad show"

Step 1 Verify if the newly logged-in user is recognized. Suppose the AD client has the IP address of 192.168.18.72 Device IP:192.168.18.92 Log out the AD user and re-login to the AD domain. Use Console / SSH / Telnet to connect to the CLI and enter the command: "sys ad show"as Fig. 1 shows, you can see the list of the registered AD clients.	 Fig. 1

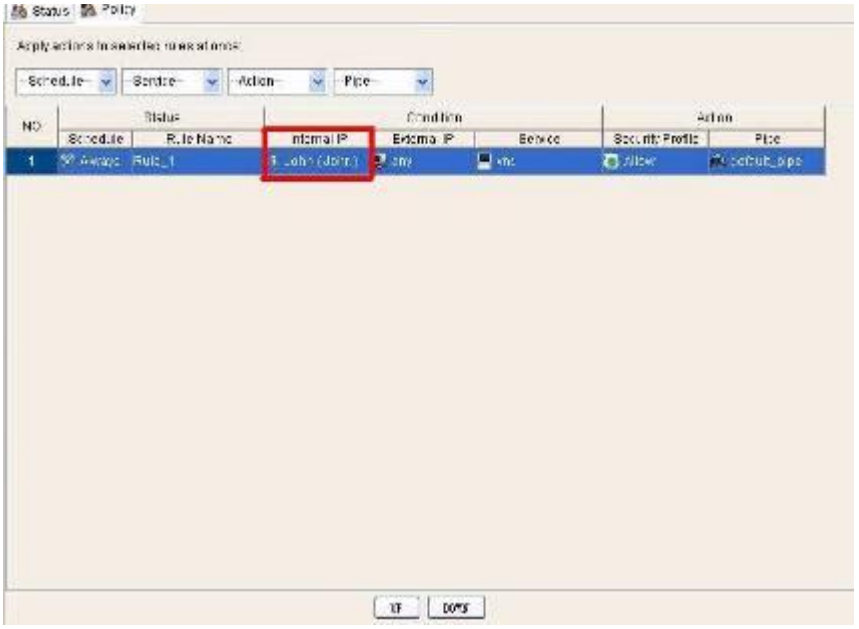
11.3.2 Map IP addresses in Reports to AD names

11.3.2.1 Import users/names from Object Manager->Dynamic Objects

Step 1. Import all accounts / names Import all accounts / names from the AD server to the UI for management. Refer to previous sections about how to	**Functions > Objects > Dynamic Objects**

fill in the User DN and the Base DN fields. After importing, all AD accounts will be listed in the "Accounts" while all AD groups will be listed in the "Group" as Fig. 1 shows.	

11.3.2.2 Assign AD user in the Policy Rules

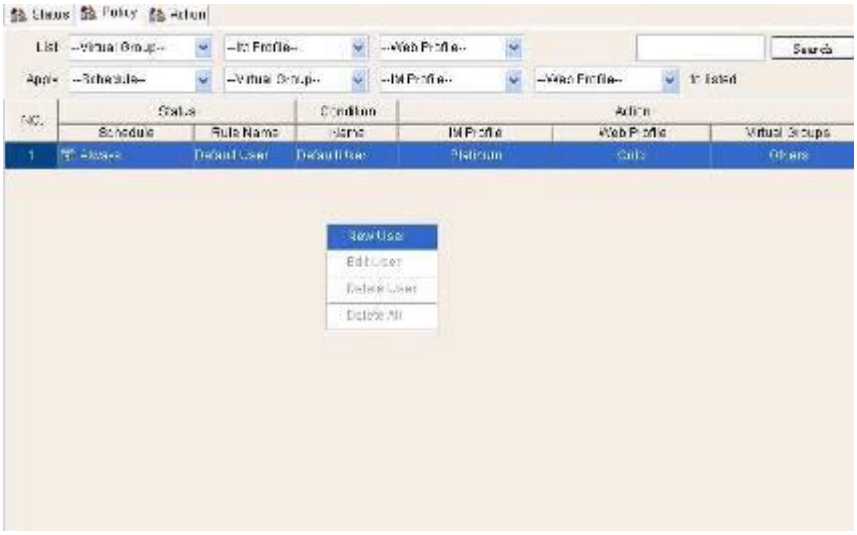
Step 1. Assign AD users in L4 Policy Rules Right click on the rule field and select "Add" to insert a new rule. Select the preferred AD user from the Internal IP and the External IP fields.	**Functions > Traffic Manager > L4 Policy > Policy** 
Step 2. Assign AD users in L7 Policy Rules Right click on one of the L7 Policy rules, select "Insert" to insert a rule before the chosen rule. Select the AD users in the Internal IP and the External IP fields.	**Functions > Traffic Manager > L7 Policy>Policy**

11.3.2.3 Assign AD users/groups in Content Policy Rules

Step 1. Insert a new rule

Right click on the empty area of the rules. Select "New User" to add a new rule for a new user / group.

Functions > Content Manager > Content Policy>Policy



Step 2. Manually assign AD user in the rule

Input the AD account in the "Name" field. For example, we input John in that field. Below the field is the permission settings for this account as shown in Fig.1. Click "Finish" to finish adding a content policy rule for the AD user "John" as shown in Fig. 2. It is the same for AD groups. Fill in the AD group name in the "Name" field.

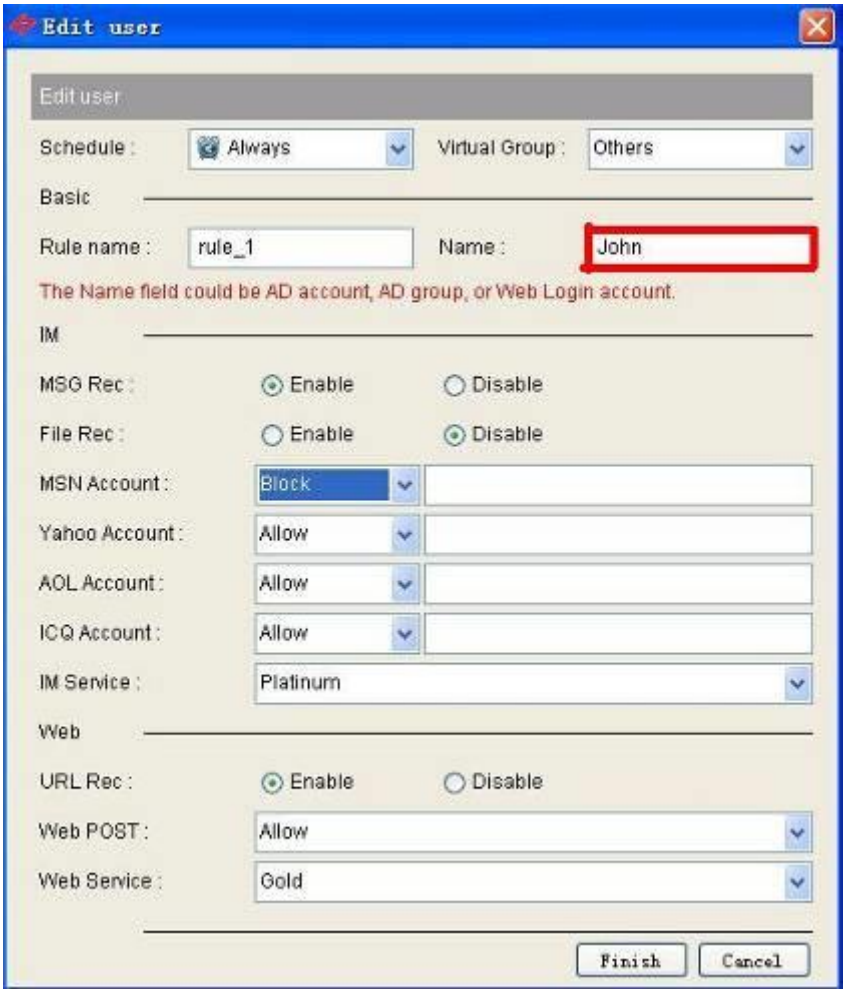


Fig. 1

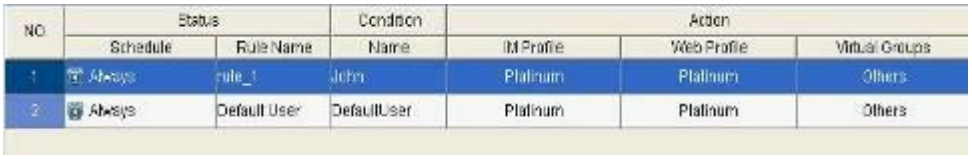
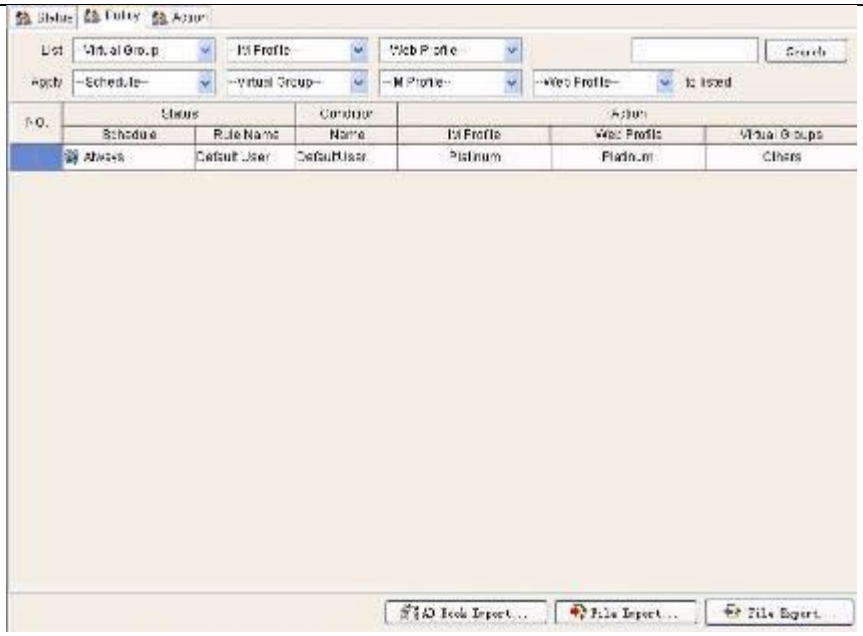


Fig. 2

11.3.2.4 Import all AD accounts from Dynamic Objects

Step 1. Click AD Import At the bottom of the Content Policy, there is a "AD Book Import". Click it to import the AD accounts or AD groups.	**Functions > Content Manager > Content Policy>Policy**



Step 3 Select AD accounts

The pop-up window allows you to select preferred AD accounts or AD groups as shown in Fig.1.

Fig.1

After you select the items and click the OK button, you can see all selected users and groups are imported as shown in Fig.2

Functions > Content Manager > Content Policy > Policy

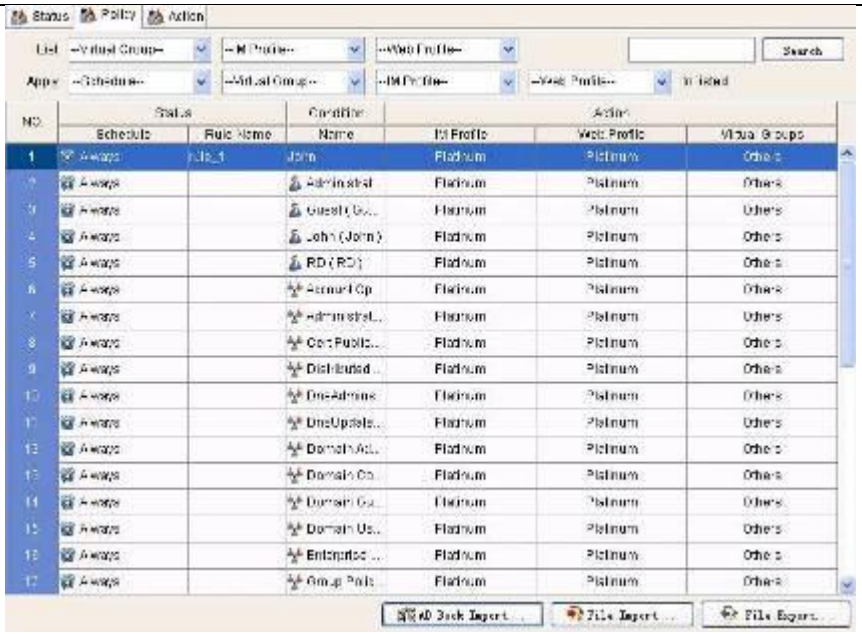


Fig.2

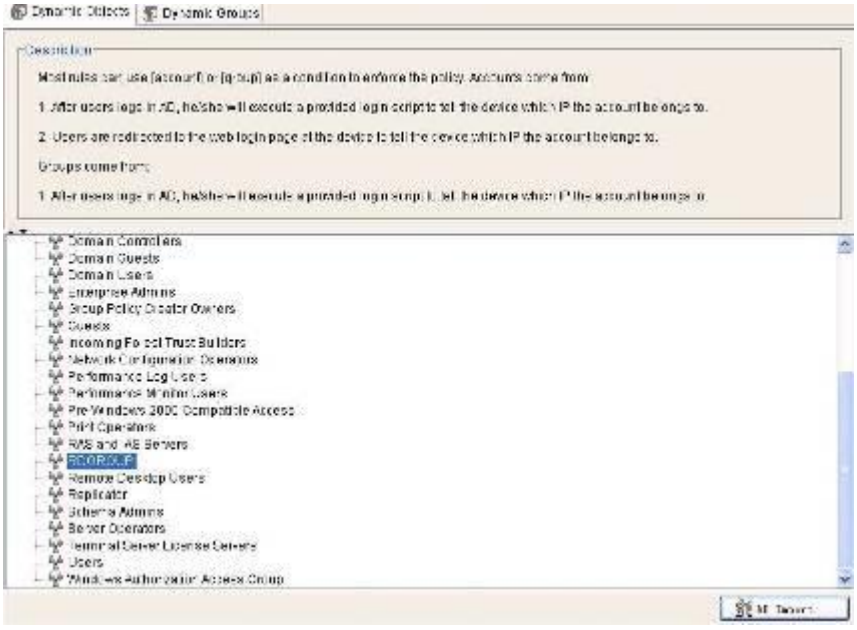
11.4 A Real Example

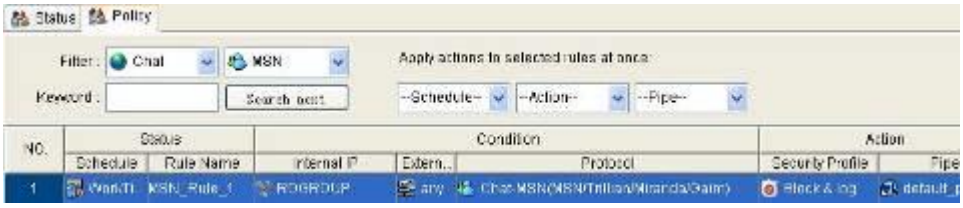
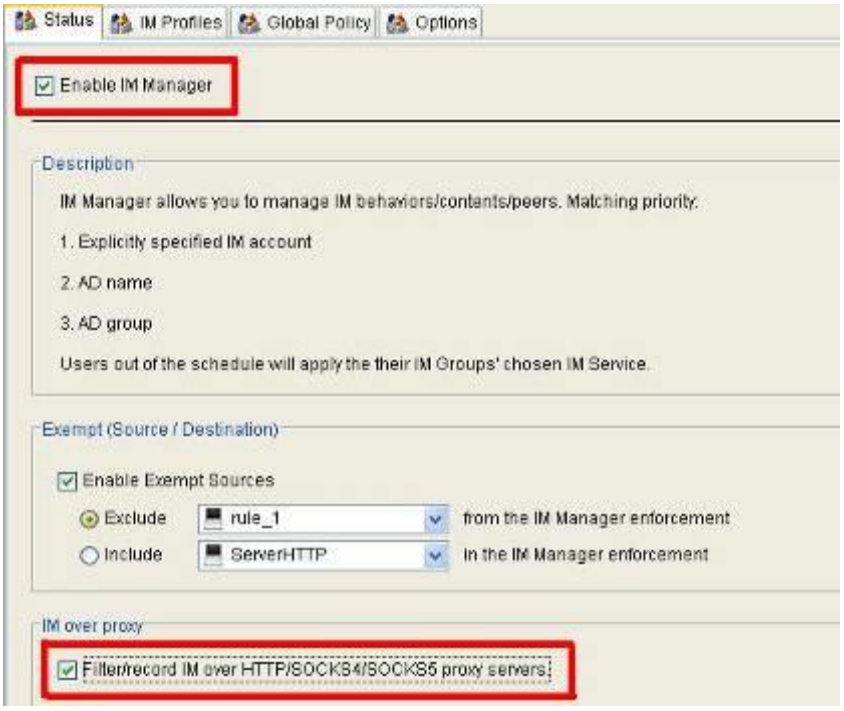
11.4.1 Manage RD People's Activities

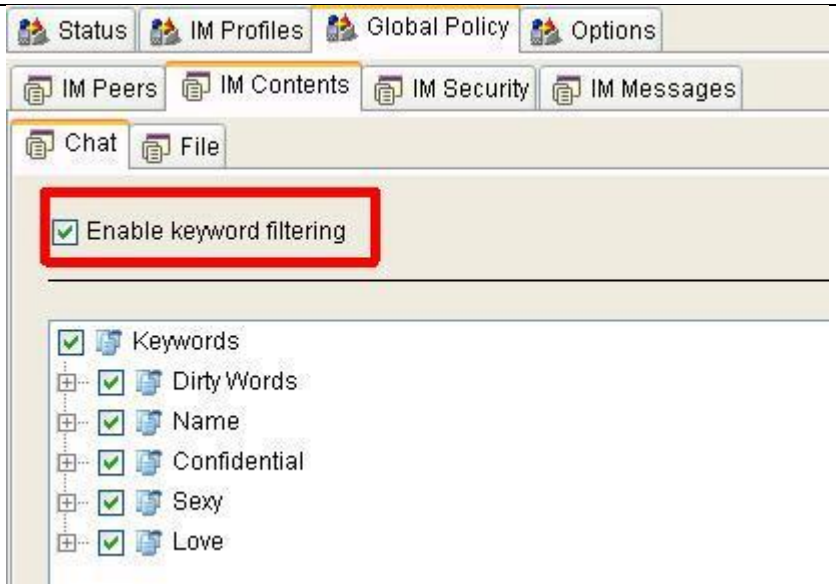
- For AD users in the RDGROUP, no MSN at office hours. They can MSN during non-office hours, but all chats will be recorded and filtered with keywords.
- For the AD user account "John", his web browsing of news, sports, and some URLs will be blocked all the time.
- For users located at the IP range of 192.168.18.20 to 192.168.18.30 will not be filtered
- Use the organization unite to group the recorded data

11.4.2 Detailed Steps

Step 1 Setup Check the original schedule.	**Functions > Objects Manager -> Static Objects > Schedule > Object** 

Step 2 Add a schedule Here we add a schedule "worktime" for the office hours	**Functions > Static>Schedule>Object** 
Step 3 Import AD accounts Go to Object Manager -> Dynamic Objects -> AD Import" to import all AD accounts and AD groups.	**Functions > Object Manager > Dynamic Object > AD Import** 

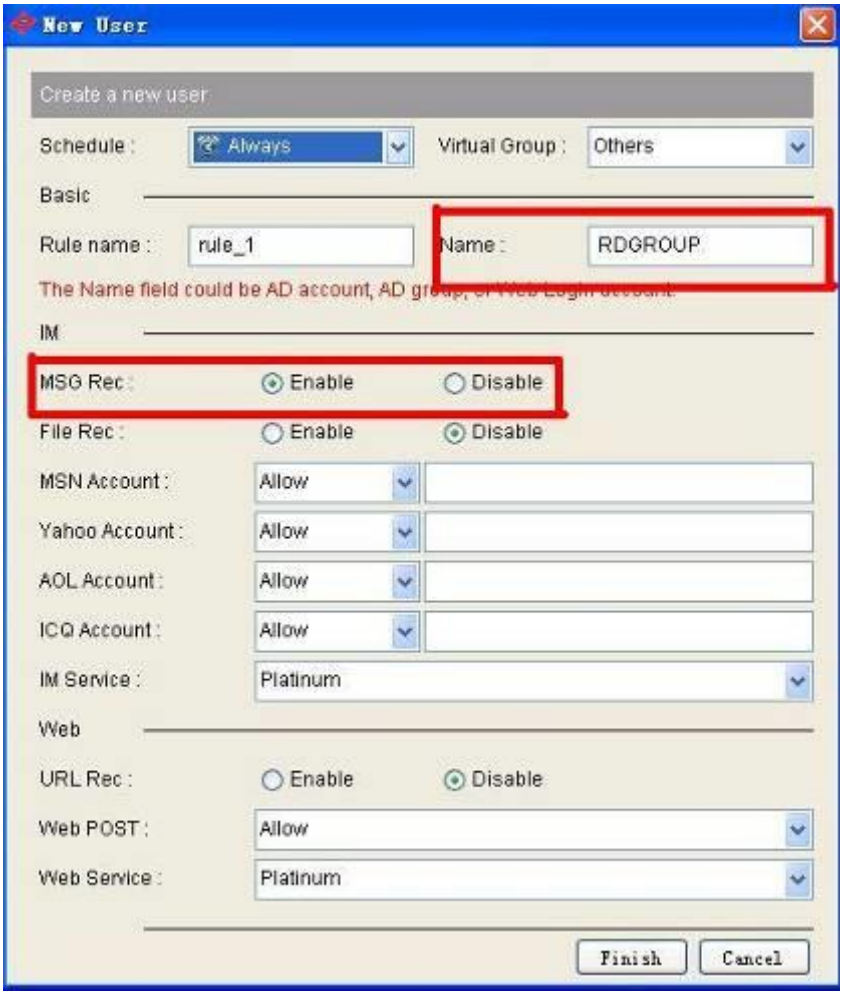
Step 4 Setup policy rules for office hours Enable the L7 Policy, and select "Chat->MSN", and select the "Worktime" in the Schedule field, and select the "RDGROUP" in the Internal IP field. Finally, select the "Block" or "Block & Log" in the Security Profile field.	**Functions > Traffic Manager > L7 Policy > Policy** 
Step 5 Setup policy rules for Non-office hours **5.1.Enable IM Manager** Select the "Enable IM Manager" and select the "Allow IM over Proxy Servers" filter the IM inside the proxy.	**Functions > Content Manager> IM>Status** 
5.2 Enable keyword Click the "Enable keyword filtering" and choose your preferred keywords in the default settings. You can add your keywords by yourself with right click on the field.	**Functions > Content Manager> IM>Global Policy>IM Content>Chat**



5.3 Create Content Policy

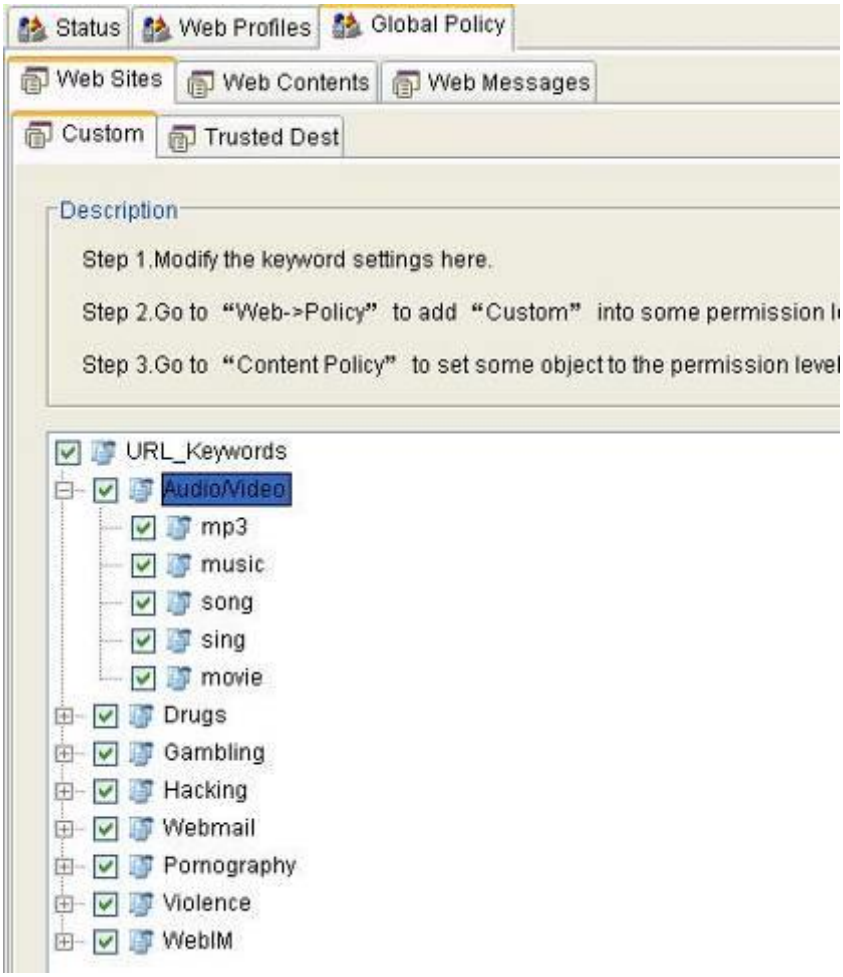
Go to [Content Policy]->[Policy] and right click on the area to choose "New User". In the "Name" field we select the "RDGROUP" and select the "Enable" in the MSG Rec field to record the MSN messages. Click the "Finish" to confirm.

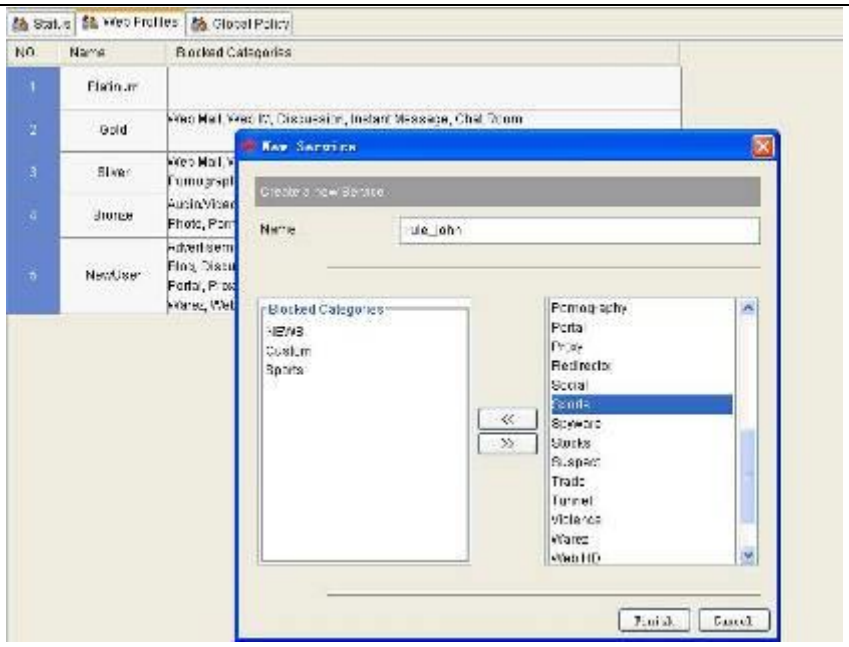
Functions > Content Manager> Content Policy>Policy



Step 6 Enable Web Manager

Functions > Content Manager> Web>Status

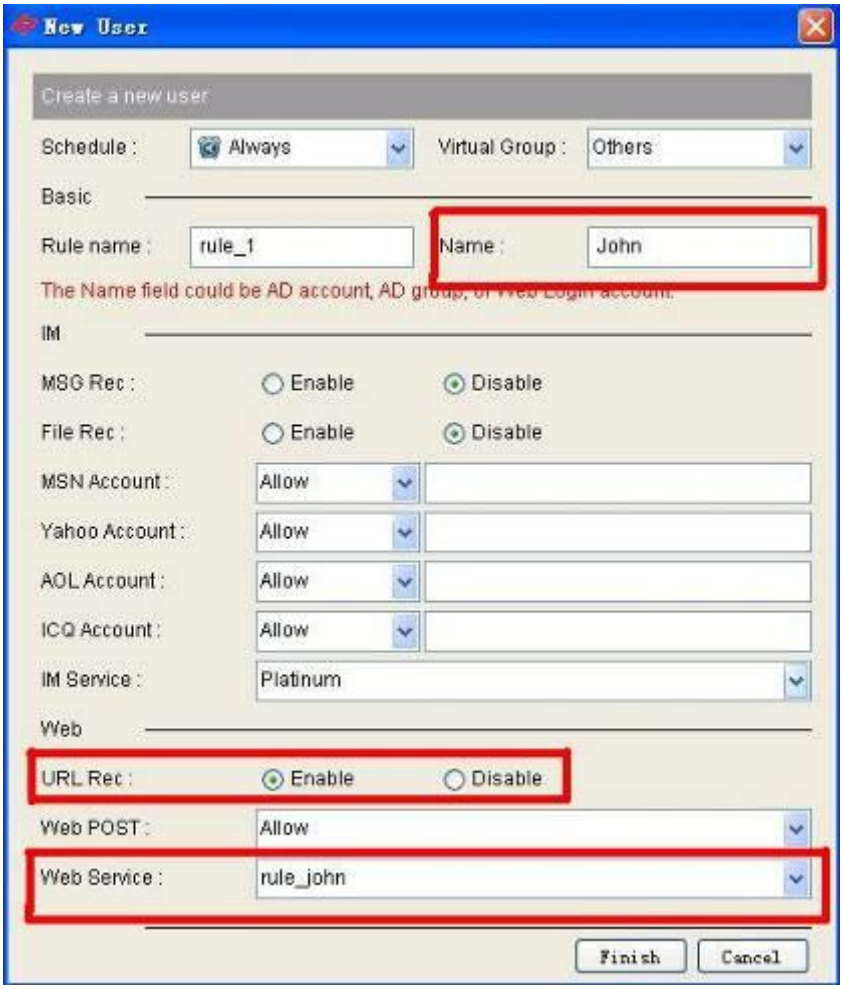
Check the "Enable Web Manger" checkbox.	
Step 7 Add custom keywords In the [Custom] tab you can add / delete / modify the keywords.	**Functions > Content Manager> Web>Global Policy>Web site>Custom** 
Step 8 Assign Web Profiles You can define a new web profile by yourself to choose your preferred categories listed in our built-in URL database.	**Functions > Content Manager> Web>Web Profiles**



Step 9 Setup John's Policy

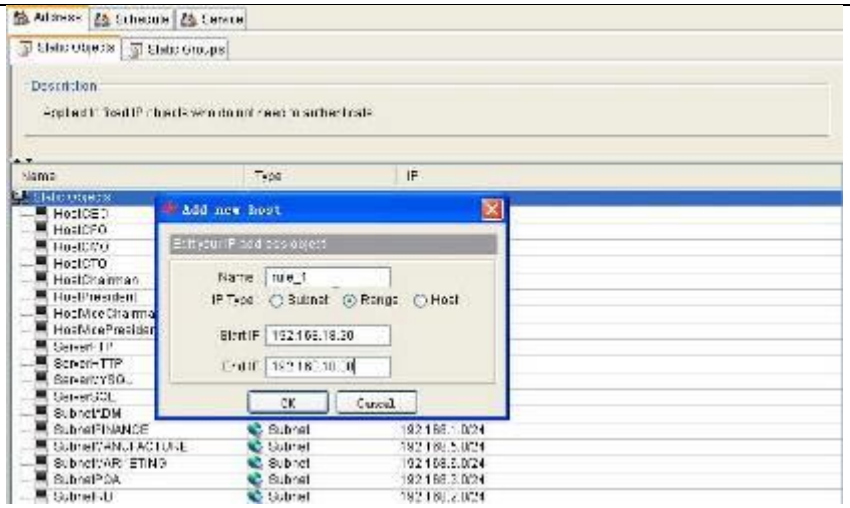
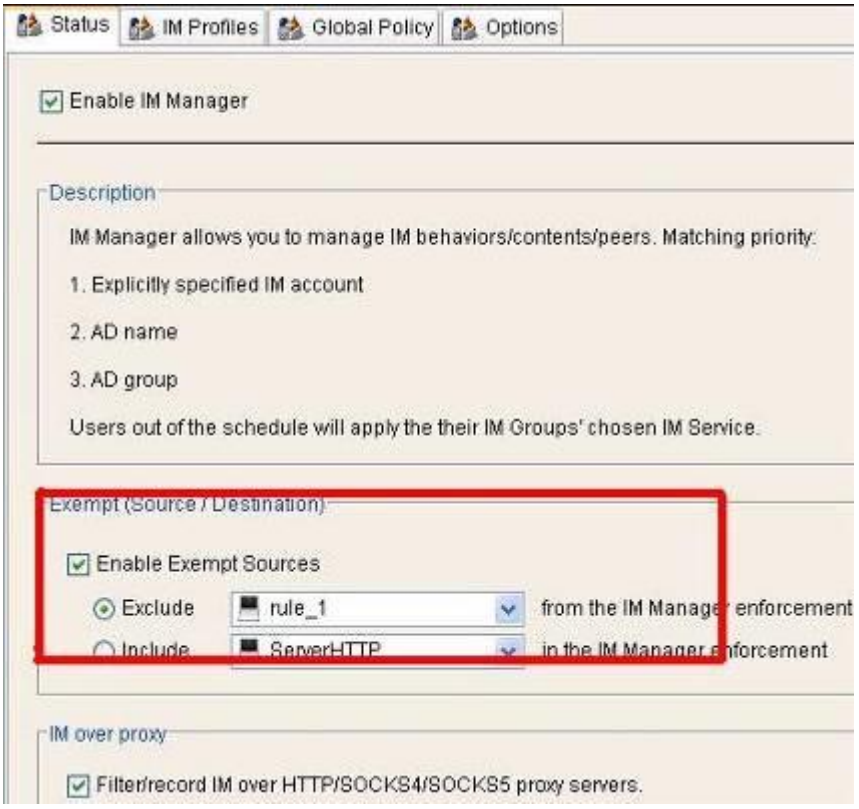
Go to [Content Policy] -> [Policy] and right click on that area to add a new user by clicking the "New User". Input "John" at the Name field and select the web profile "rule_john" which was just created in the previous step. Check the "URL Rec" to record the visted URLs by John.

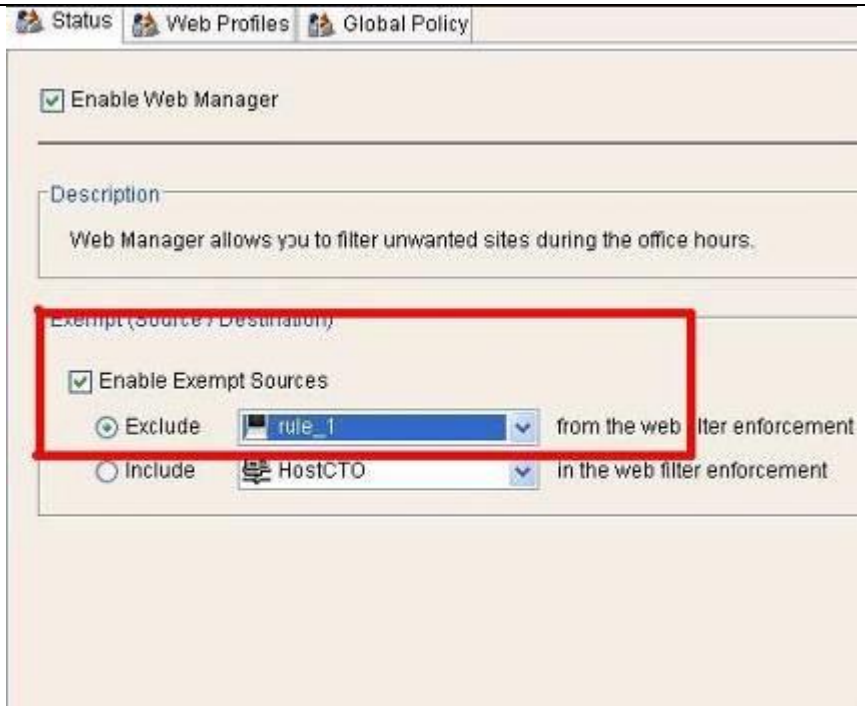
Functions > Content Manager> Content Policy >Policy



Step 10 Create IP Groups

Functions > Object Manger> static> Address>Static Object

Go to [Object Manger] -> [Static] -> [Address] -> [Static Objects] and right click on the tree root or any tree node of the tree. Select the "Add" in the pop-up meu and give a meaningful name in the "Name" field. Select the "Range" and input "192.168.18.20" in the "Start IP" field and input the "192.168.18.30" in the "End IP" field. Click the "OK" button.	
Step 11 Exclude Specific IPs Check the "Exempt (Source / Destination)" option and select the "Exclude" option to enter the host "rule_1".	**Functions > Content Manager> IM >Status**  **Functions > Content Manager> Web>Status**



Step 12 Use OU to store the private data in AD tree

As long as you assign the AD group or your manually created virtual group in the OU field, users' private logs will be put under the OU.

First, right click on the "Organization Units" and select "Add Group" to create a virtual group. In this example, we add a virtual group named "AE" as shown in Fig. 1.

Next, select the "AE" in the OU field in the rule "rule_1" as shown in Fig. 2.

Next, right click on the rule and select "Edit User" to enter the dialogue as shown in Fig. 3.

Functions > Content Policy> Action

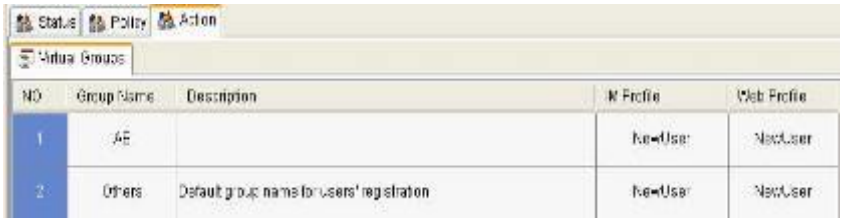


Fig. 1

Functions > Content Policy> Policy

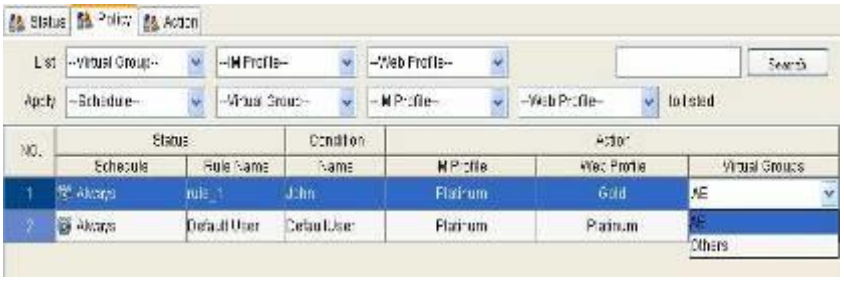


Fig. 2

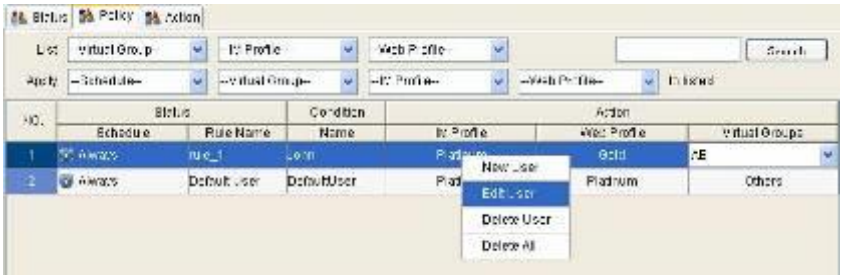


Fig. 3

Enable the MSG Rec to enable the recording of chat messages as shown in Fig. 4.

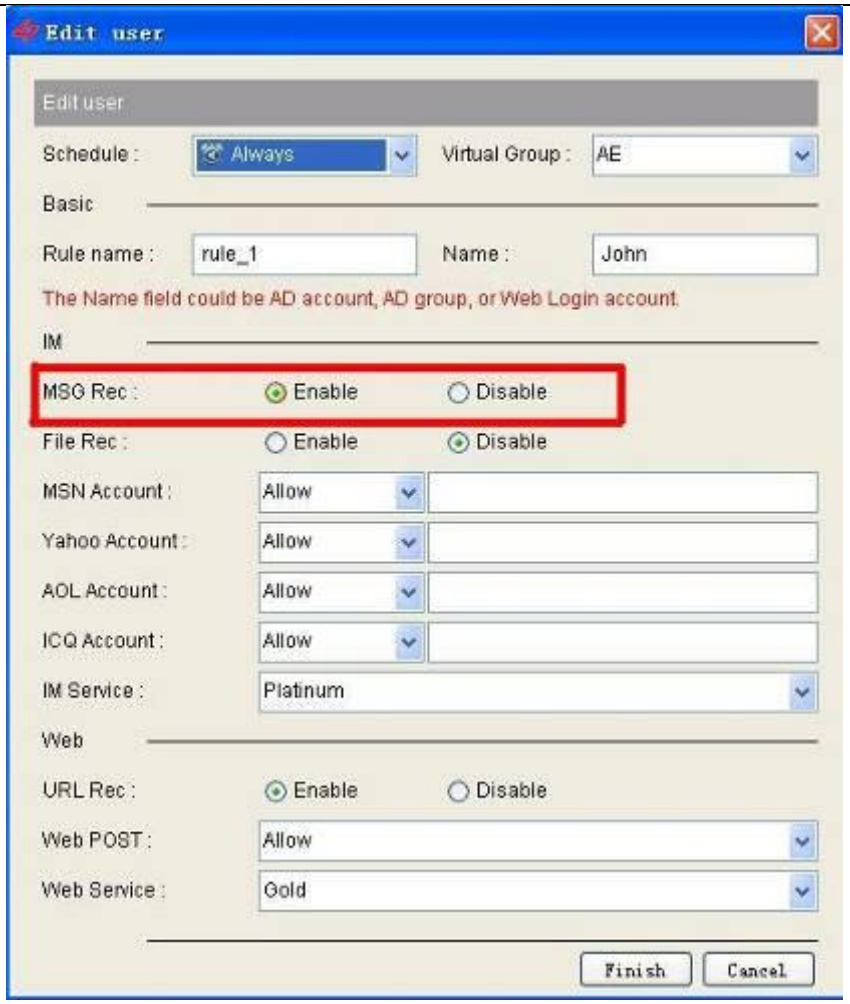


Fig.4

Relogin the AD client "John" to the AD domain and use the account to login to his MSN account to chat. Then we can see that all John's chat messages are logged into the OU "AE" as shown in Fig. 5.

Functions > Recoder> IM

Fig. 5

Chapter 12
Web Manager

This chapter introduces how to use Web Manager to manage your employee's HTTP traffic

12.1 Scenario

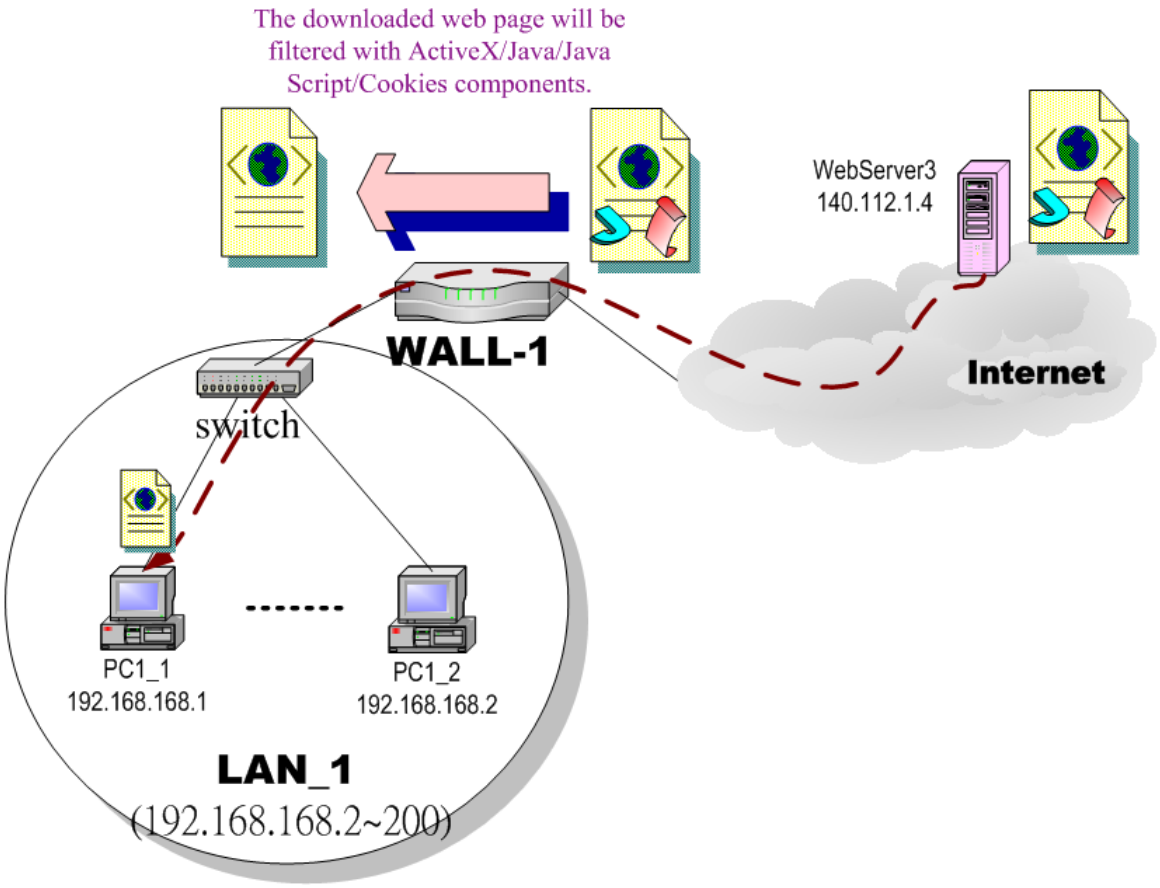


FIGURE 12-1 Prevent employees from accessing illegal websites.

1. As described in FIGURE 12-1, the user PC1_1 is browsing the website located at the WebServer3. The content of the website contains cookies, Java applets, and ActiveX objects. These contents may contain malicious code that may steal the private information of the user. So the administrator decides to disallow users to download the objects to PC1_1.

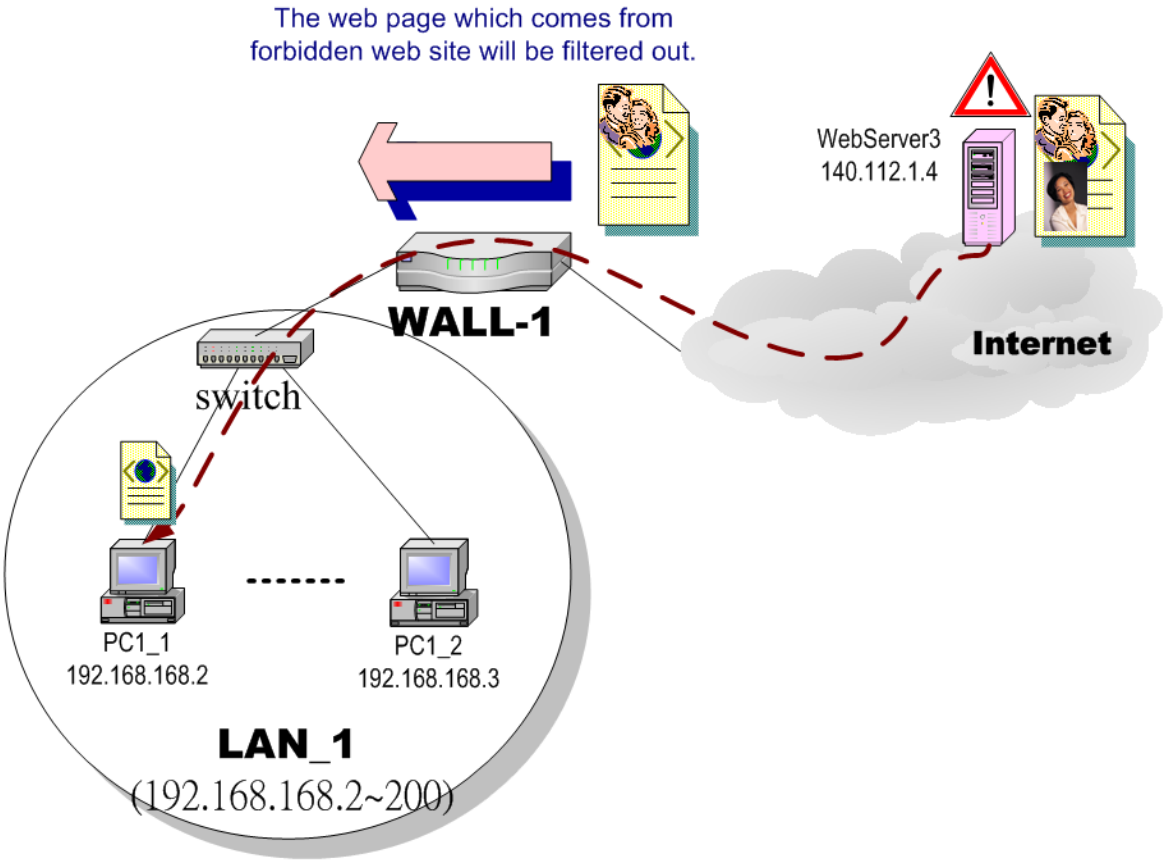


FIGURE 12-2 Denying access to illegal websites through web filtering

2. As described in FIGURE 12-2, the user PC1_1 is browsing websites that contains stock information, violence, or even sex. Some websites may contain video or audio which may waste the Internet bandwidth of the company. What is worse, the contents may lower the productivity of your employees.

12.2 Objectives

1. Block HTTP objects such as cookies, Java applet, and ActiveX from web pages.
2. Disallow employees from visting illegal websites.

12.3 Methodology

1. Setup web objects to filter cookies or Java applets.
2. Setup the web filter to block websites by URL. The URL filter can be setup to analyze by URL keywords or built-in URL database. Traffic matching the URL will be blocked.

12.4 Steps

Step 1 **Enable Web Filter**

Check the **Enable Web Filter** to enable the web filter.

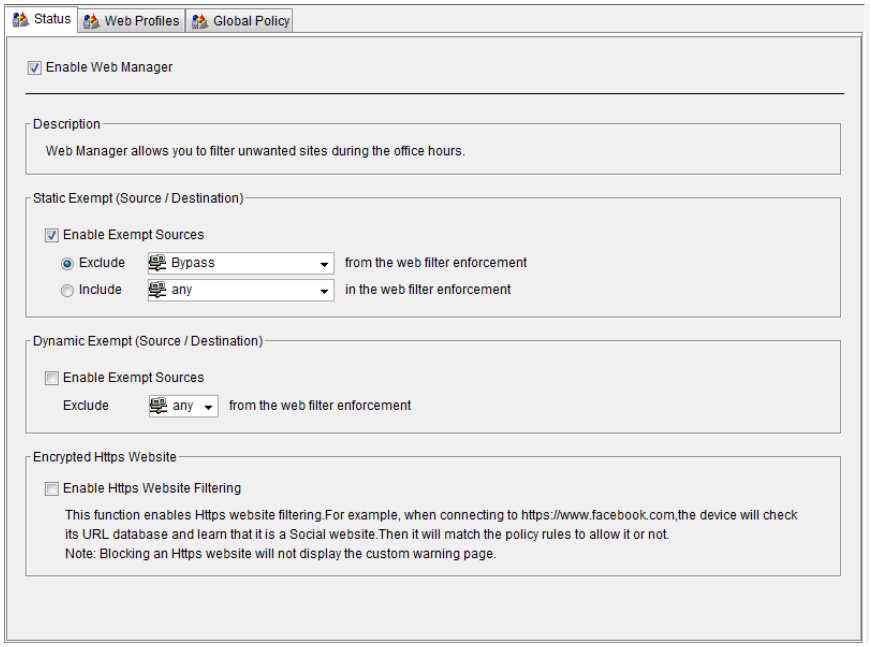
Note that when you enable the function, all port 80 http requests will be processed by the web filter. The HTTP responses are not processed becaused of performance and compatibility issues.

Step 2 **Define exempt sources**

You can define the IP range to apply the web filter function. By default, the function will apply on all computers.

Select Boss in the Exclude to **Exclude Boss from web filter enforcement.**

Functions > Content Manager > Web > Status



Field	Description	Range / Format	Example
Enable Exempt Sources	Enable the exempt source function	Enable / Disable	Enable
Exclude ____ from the web filter enforcement	Exclude the selected users to apply the web filtering functions. All other computers are enforced to do web filtering.	Enable / Disable	Enable / Boss
Include ___ in the web filter enforcement	Include the selected users to apply the web filtering functions. All other computers are not enforced to do web filtering.	Enable / Disable	Disable

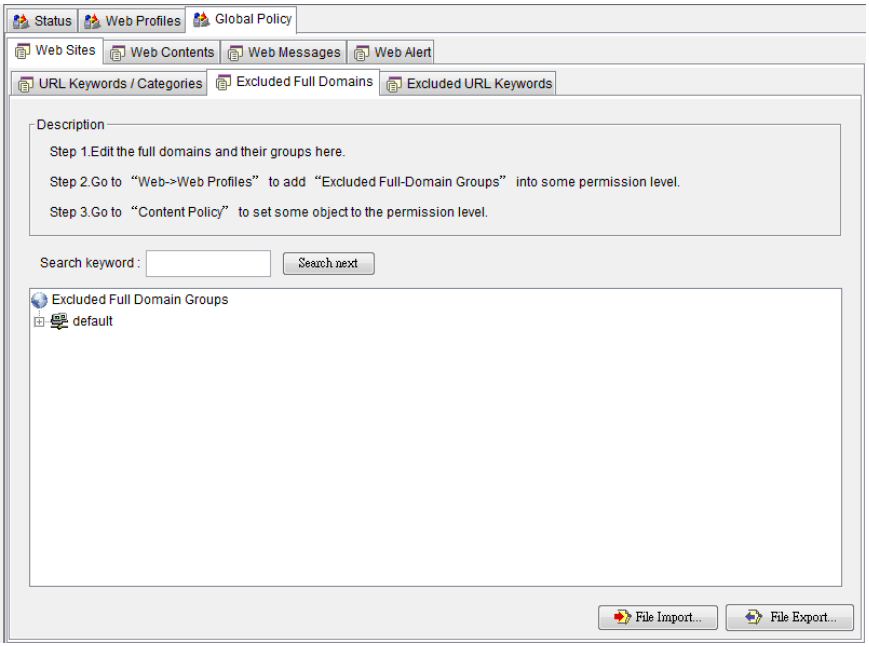
FIGURE 12-1 Exempt source fields

Step 3 **Define Excluded Domains**

Edit the **Excluded Full Domains** to add trusted domains and their groups.

Input the trusted domain by right clicking the group name. Note that entering too many domains will slow down the network performance.

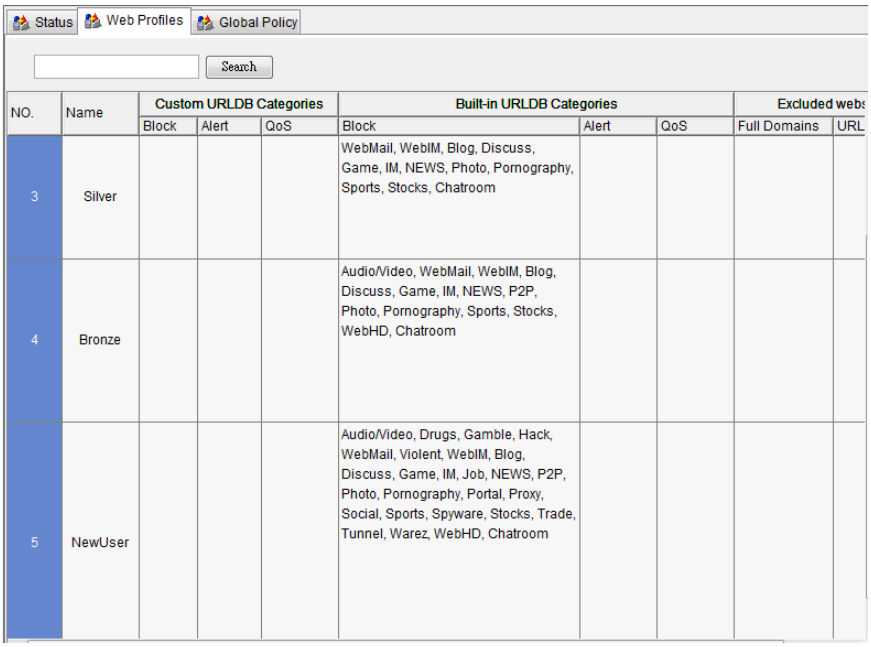
Functions > Content Manager > Web > Global Policy > Web Sites > Excluded Full Domains



Step 4 **Enable URL database**

Check the **Enable URL Database** to use the built-in URL database. You can select the categories of the URLs and the actions to apply when the product matches the URL.

Functions > Content Manager > Web > Web Profiles



Field	Description	Range / Format	Example
Enable URL Database	Enable URL database to block URLs	Enable / Diable	Enable
Action	Action to take when the URL matches the URL database.	Log Only / Log & Block / Block Only	Log & Block

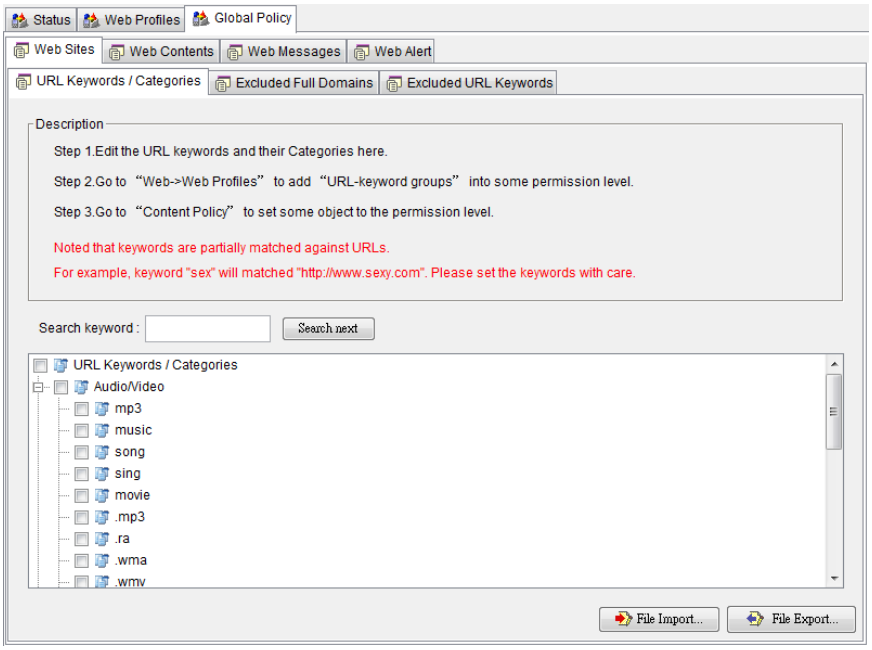
Categories	Enable all categories.	Enable / Diable	Disable
Block all categories	Block URLs that match anyone of the URL categories.	Enable / Diable	Disable
Advertisements/Audio/Video/Drugs etc	Check the URL categories to be enforced.	Enable / Diable	Enable

FIGURE 12-2 URL Web filtering fields

Step 5 **URL keyword blocking**

Check the **Enable URL Keyword blocking** to block any URL containing the keywords listed in the settings. The product has preset keywords. You can change the keywords by right clicking the item.

Functions > Content Manager > Web > Global Policy > URL Keywords / Categories



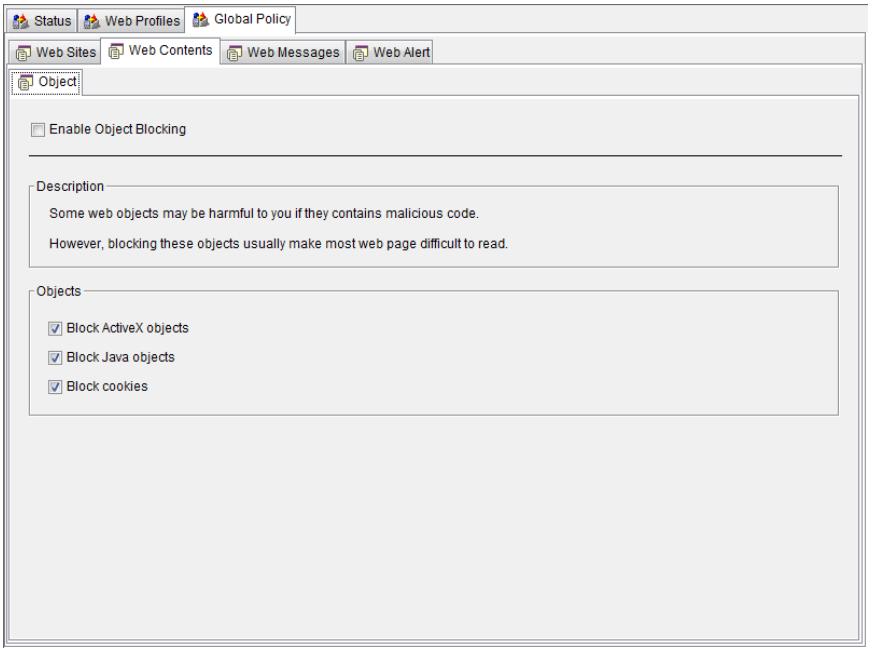
Field	Description	Range / Format	Example
Enable URL Keyword blocking	Enable the URL keyword blocking.	Enable / Disable	Enable
URL Keywords	If you want to browse some URL which has keywords in the list, your browsing will be stopped.	String	Adv/advertise/adsrv/ banner/splash

FIGURE 12-3 URL keyword filtering

Step 6 **Web Objects**

Check the **Enable Object Blocking** and select the objects to block in all incoming web objects.

Functions > Content Manager > Web > Global Policy > Web Contents



Field	Description	Example
ActiveX	Filter web pages with ActiveX objects.	Enable/Disable
Java	Filter web pages with Java objects.	Enable/Disable
Java Script	Filter web pages with Java Script objects.	Enable/Disable
Cookies	Filter web pages with Cookies objects.	Enable/Disable

FIGURE 12-4 Web object filtering

Field	Description	Range / Format	Example
Enable Keyword Blocking	Enable URL keyword blocking	Enable / Diable	Enable
Keywords	Input the keyword that may appear in the URL.	Keyword pattern	adv advertise adsrv banner splash

FIGURE 12-5 URL keyword blocking fields

Chapter 13
Encryption Web Manager

This chapter introduces how to use Encryption Web Manager to manage your employee's HTTPS traffic

13.1 Scenario

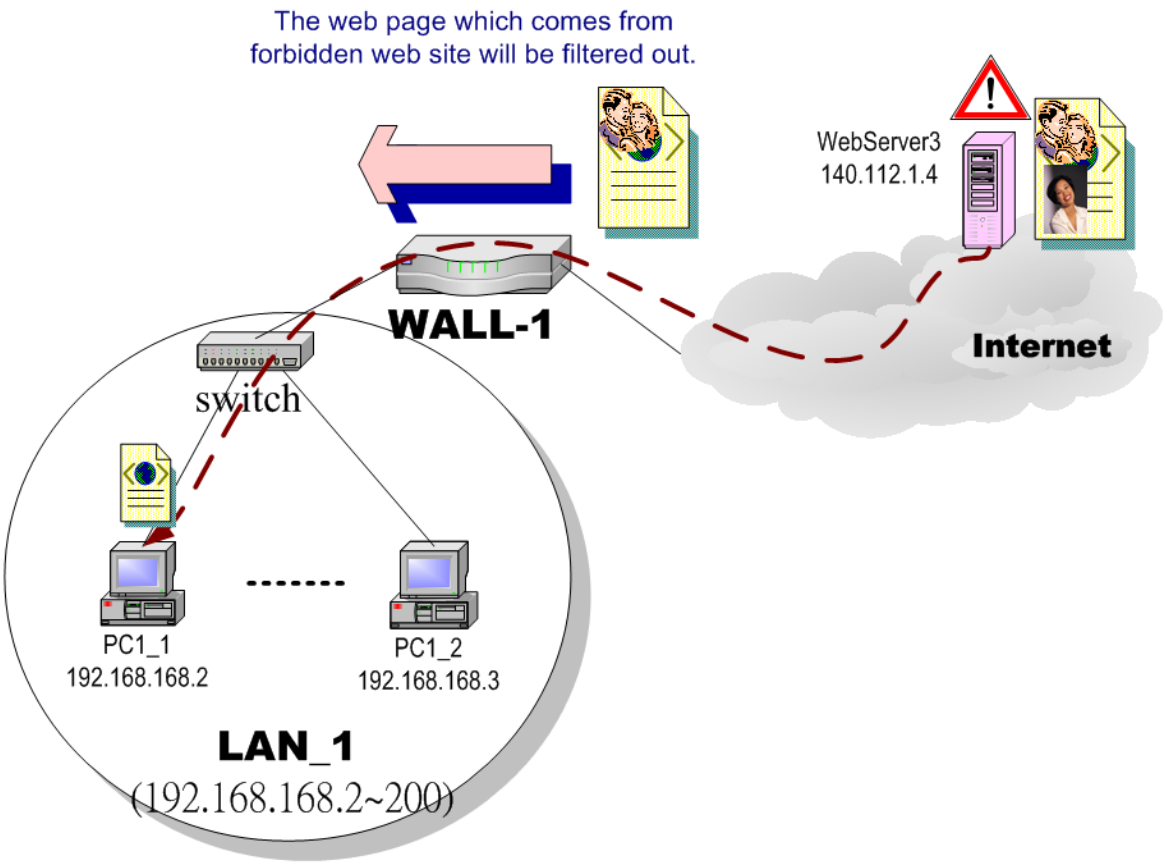


FIGURE 13-1 Denying access to illegal websites through web filtering

1. As described in FIGURE 12-2, the user PC1_1 is browsing websites that contains stock information, violence, or even sex. Some websites may contain video or audio which may waste the Internet bandwidth of the company. What is worse, the contents may lower the productivity of your employees.

13.2 Objectives

3. Disallow employees from visting illegal websites.

13.3 Methodology

1. Setup the web filter to block websites by URL. The URL filter can be setup to analyze by URL keywords or built-in URL database. Traffic matching the URL will be blocked.

13.4 Steps

Step 1 **Enable Encryption Web Recorder**

Check the **Enable Encryption Web Recorder** to enable the SSL decryption over https..

Functions > Encryption Recorder > Web > Status

Step 2 **Define exempt sources**

You can define the IP range to apply the web filter function. By default, the function will apply on all computers. You can include specific traffic into this manager or exclude specific traffic from this manager.

Select Boss in the Exclude to **Exclude Boss from web filter enforcement.**

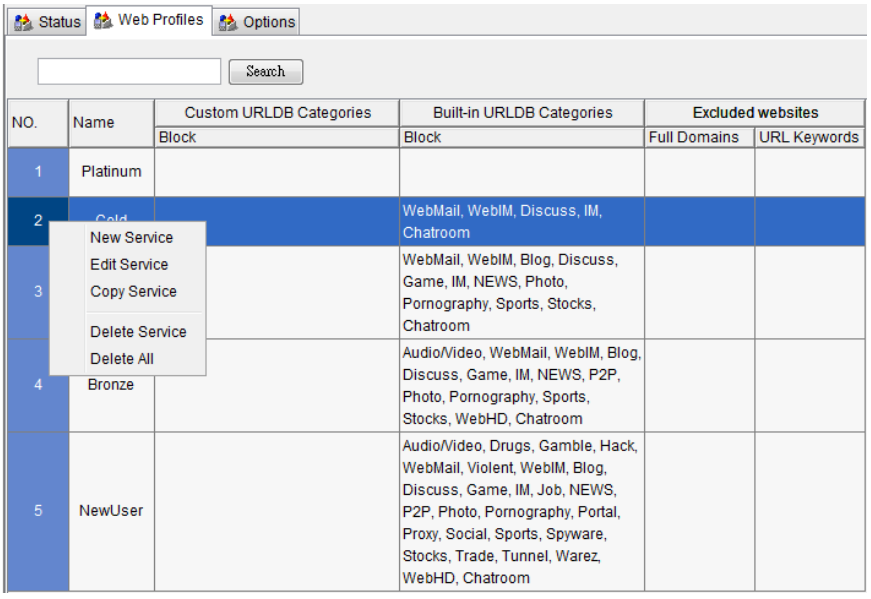
Field	Description	Range / Format	Example
Enable Exempt Sources	Enable the exempt source function	Enable / Disable	Enable
Exclude ____ from the web filter enforcement	Exclude the selected users to apply the web filtering functions. All other computers are enforced to do web filtering.	Enable / Disable	Enable / Boss
Include ___ in the web filter enforcement	Include the selected users to apply the web filtering functions. All other computers are not enforced to do web filtering.	Enable / Disable	Disable

FIGURE 13-1 Exempt source fields

Step 3 **Define Web Profiles**

Edit the profile you want to apply to the users. Right click at the row you can choose to new / edit / copy / delete the service profile.

Encryption Recorder > Web > Web Profiles



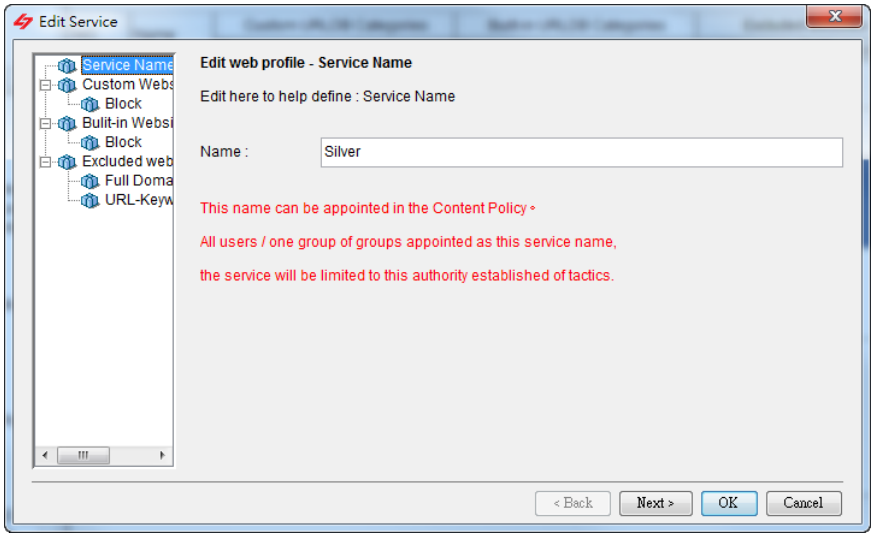
Step 4 **Edit service profile**

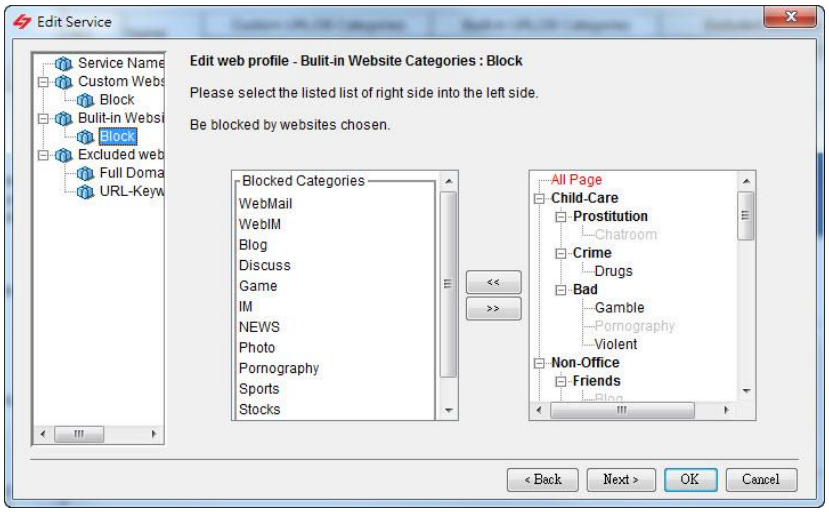
Choose “Block” from the Built-in Website Categories in the leftmost tree. You can see a lot of categories of the built-in URL database.

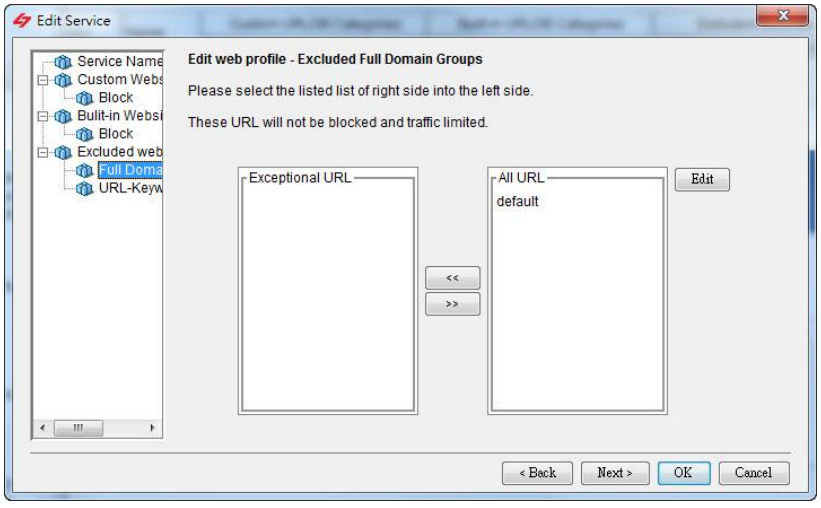
Select the categories you want to block. For those categories already selected to the left side, they are in grey / disable state at the right side and cannot be selected again. When users visit the websites in those selected categories, they will be blocked.

However, the built-in database of custom URL keywords may accidentally block the wrong websites. You can edit the **Excluded websites** by editing the **Full Domain Groups** or **URL-Keyword Groups**.

Encryption Recorder > Web > Web Profiles







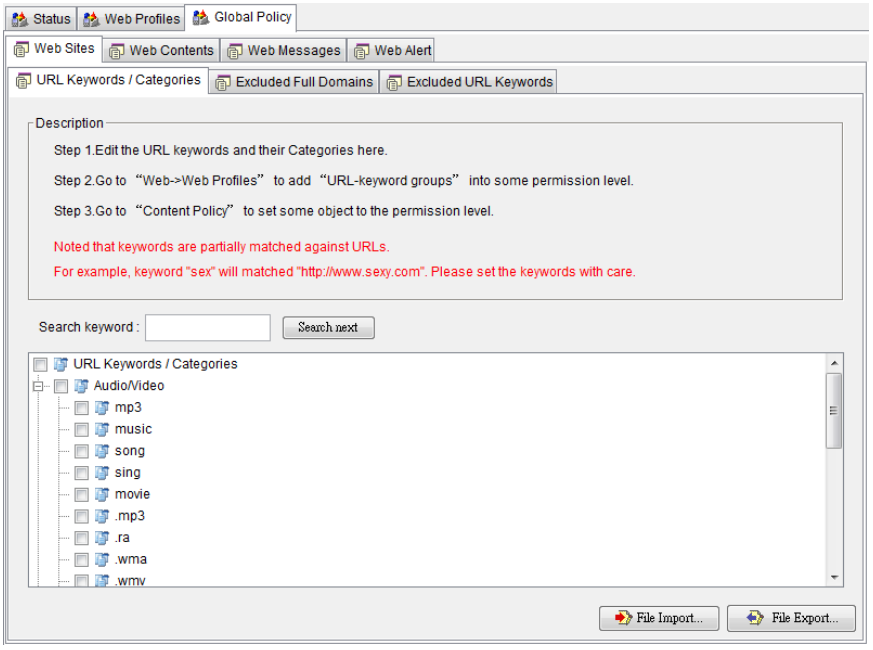
Field	Description	Range / Format	Example
Enable URL Database	Enable URL database to block URLs	Enable / Diable	Enable
Action	Action to take when the URL matches the URL database.	Log Only / Log & Block / Block Only	Log & Block
Categories	Enable all categories.	Enable / Diable	Disable
Block all categories	Block URLs that match anyone of the URL categories.	Enable / Diable	Disable
Advertisements/Audio/Video/Drugs etc	Check the URL categories to be enforced.	Enable / Diable	Enable

FIGURE 13-2 URL Web filtering fields

Step 5 **URL keyword blocking**

Check the **Enable URL Keyword blocking** to block any URL containing the keywords listed in the settings. The product has preset keywords. You can change the keywords by right clicking the item.

Functions > Content Manager > Web > Global Policy > URL Keywords / Categories



Field	Description	Range / Format	Example
Enable URL Keyword blocking	Enable the URL keyword blocking.	Enable / Disable	Enable
URL Keywords	If you want to browse some URL which has keywords in the list, your browsing will be stopped.	String	Adv/advertise/adsrv/ banner/splash

FIGURE 13-3 URL keyword filtering

Field	Description	Range / Format	Example
Enable Keyword Blocking	Enable URL keyword blocking	Enable / Disable	Enable
Keywords	Input the keyword that may appear in the URL.	Keyword pattern	adv advertise adsrv banner splash

FIGURE 13-4 URL keyword blocking fields

Part 6

System Maintainence

Chapter 14
Mangement Server Maintainence

This chapter introduces how to use mailer to achieve auto system maintainence & alerts

14.1 Introduction to Management Server

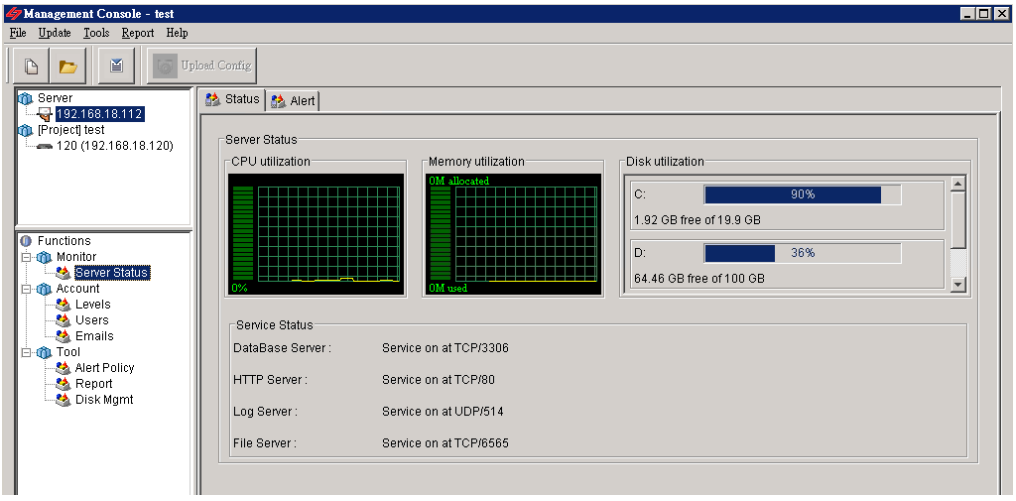
Management server is a software to do centralized configuration mangement and log server of many devices. It can be a standalone installation on a Windows based machine or a built-in server software module of the gateway product.

- **Server Status:** Check the current status of the CPU & memory, and the on/off status of each software modules such as MySQL database, apache web server and their installation directory.
- **Email Alerts:** Setup the email server and customized email alert contents.
- **FTP Backup:** Setup the FTP server for the mailer to backup the data to.
- **Scheduled Reports:** Setup the time, receiver, and format for the scheduled email report.
- **System Alerts:** Setup the severity level of the system alerts.

Detailed configuration descriptions are listed below.

14.2 Configuring the Management Server

After you have installed the management server and rebooted the server, there will be a small icon at the right bottom corder of the management server. Please double click the icon.

Step 1 System Information	**Monitor > Server Status**
In this page you can see the CPU / memory usagestatus of the management server. You can also find the directory of each software module.	

Step 2 Setup Email Server Click the **Edit** button and select the the **By Local Server** option. Input the IP address of the **DNS Server**. If you want to alert the administrator by SMTP email, please check the **By SMTP Server** option. Either the two ways of sending the email should be tested to verify that if it really works with your preferred server. You can test it by clicking the **Test** button. If it works, you can then decide to enable the email alerts or not by checking the **Enable / Disable Mail Alert**. If enabled, input the **Check Period (min)** field so that the program will check if there are any message it should alert every that periold.	**Monitor > Server Status**
Step 3 Customized Email Message Move the cursor at the text input area and click it. You can use the variables $Date, $App, $Action, $User to compose your email contents.	**Monitor > Server Status**

Variable	Description	Example
$Date	The date when the policy violation occurs.	2005/01/01 10:10:00
$App	The IM application name of the policy violation event	MSN
$Action	The IM activity of the policy violation event	file transfer
$User	The IM account of the policy violation event	user@host.your.com

FIGURE 14-1Alert email variables

Step 4 FTP Setup At the FTP Setup page, you can use FTP to do backup. Check the **Enable FTP Backup**, and check the **Backup only** option. You can then choose the FTP backup schedule by a daily basis, weekly basis, or monthly basis. Input your exact time to backup the data in the pop-up dialog. For example, click the **Daily** button, then select **15:00** to ask the system to back the data every day at 15:00.	**Monitor > Server Status**

Step 5 Choose Backup Type In the **Backup Type** area, choose your preferred style of backup. When you want to restore your data, please click the **Get Bakup List** button and select the directory of the FTP server where the backup file is located. Click the **Restore** to start restoring the data.	**Monitor > Server Status**
Step 6 FTP Server settings Check the **Edit** to start editing related settings. Input 始 the IP address, account, and password of the FTP server. Check the PSV if you want to use passive mode FTP. Click the Test to test the connectivity of the FTP server. Check the Save button to store related options. As said in the above, you can choose to back the log at 3:00 PM everyday. The system will auto backup the log at that time. All backup directory will be named by the date.	**Monitor > Server Status**
Step 7 Reporting system Check the **Edit** button to start editing related settings. Select the the period to send the report (daily / weekly / monthly). Check the format you want to receive (PDF/HTML/Excel) and which devices you want to know. Input the email address of the receiver and click the Save button to save all your inputs. **Note:** before you setup the report center, please make sure that you have chosen the report items. Otherwise, you may get an empty report.	**Monitor > Server Status**
Step 8 Syslog record Check the **Edit** button to start editing related settings. Check the **Enable/Disable Send Syslog By E-mail** and input your email address in the field. Drag the mouse to the level you want know. There are five levels: (1) Alert (2) Critical 3) Warning (4) Notification (5) Information. If you want to receive alerts only in the Alert level, you can drag the bar to the **Alert**. However, if you want to receive all the system logs, you must position the bar to the **Information**. Click the **Test** button to test the email address. Click **Save** to save all the settings.	**Monitor > Server Status**
Step 9 Version Here you can refer many version information.	**Monitor > Server Status**
Step 10 Clear / Store system logs Right clicking the status area makes you store the records to the disk.	**Monitor > Server Status**

Chapter 15
System Maintainence

This chapter describes how to upgrade firmware and backup/restore configurations

15.1 Scenario

1. The device allows you to upgrade firmware and pattern / URL database. This chapter introduces you how to upgrade the firmware through the TFTP server.

2. When the configuration is damaged, you can reset the system back to factory defaults at the CLI interface. When you forget the password, you are only allowed to enter the emergency mode to reset the configuration.

3. After you have configured the system, you can backup the configuration in case you need to restore the settings.

15.2 Upgrade Firmware through TFTP

FIGURE 15-1 Upgade firmware from TFTP server

Step 6 **Setup a TFTP server** Place a TFTP server program at the root directory such as C:\. Place firmware file with extension bin at the root directory of the TFTP server. Setup the PC to be at the same subnet of the device management port. Enter “en” to enter the priviledged mode.	
Step 7 **Upgrade firmware** Enter the “ip tftp upgrade image <FILENAME> 192.168.168.170”. After that, the device will reboot right away. However, make sure the upgrade is successful without any errors such as checksum error. After reboot, enter the CLI and use “sys ver” to check the version of the system.	InstantScan# ip tftp upgrade image IS-50-2.0.02.bin 192.168.168.170 Fetching from 192.168.168.170 or IS-50-2.0.02.bin Upgrading... System will reboot now Press ctrl+e in 5 secs to start with emergency kernel. Booting. Checking Initial Key of this device.....[OK] InstantScan login:

Step 8 **Check version after upgrade**

After rebooting the system, please check if all version & settings are correct.

```
InstantScan login: admin
Password:
Welcome to InstantScan...
InstantScan> en
InstantScan# ip show
  ================================================================================
  Gateway: 192.168.168.254
  Primary DNS: 168.95.1.1
  Secondary DNS: 0.0.0.0
  Management Server: 10.1.1.10
  ================================================================================
  Port Interface IP Address       Netmask          Status
  ---- --------- ---------------- ---------------- --------------------------
    1   INTERNAL     N/A              N/A          UP
    2   EXTERNAL     N/A              N/A          UP
    3      MGT    192.168.168.201  255.255.255.0    UP
    4      HA          N/A              N/A          DOWN (HA Disabled)
  ================================================================================
InstantScan#
```

15.3 Backup Config

Step 1 **Backup configuration**

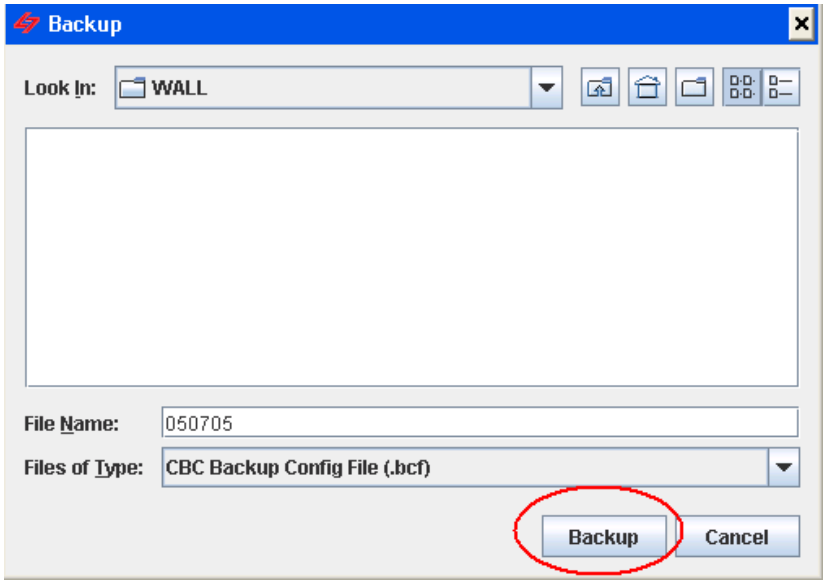
Click the **Tools** in the menu and check the **Config Backup**。

Tools > Config Backup

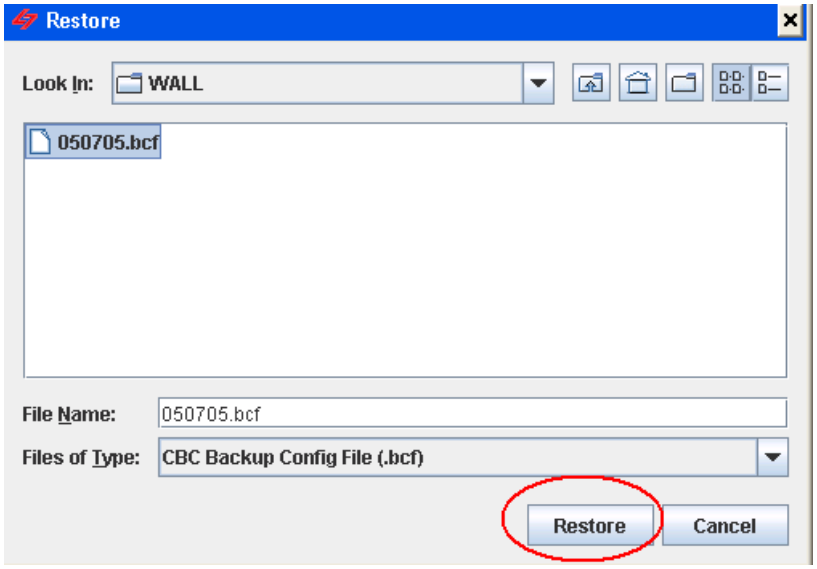
Step 2 **Store the backup config**

Select the directory you want to store the backup file. Input the filename and click the **Backup** to finish the backup.

Tools > Config Backup



15.4 Restore Config

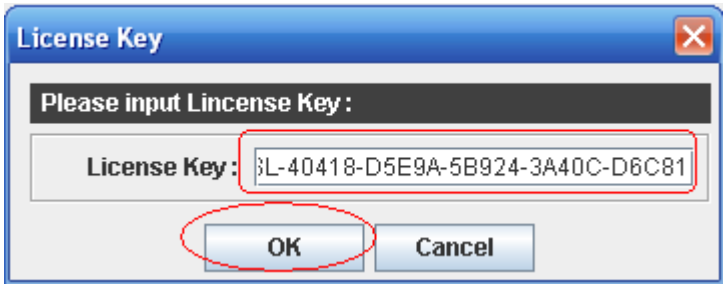
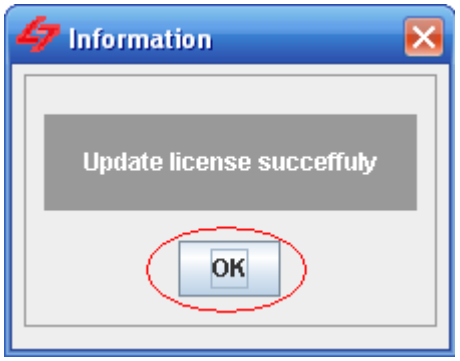
Step 1 **Restore configuration** Click the **Tools** in the menu and check the **Config Restore**.	**Tools > Config Restore** 
Step 2 **Select the config to restore** Please select the config file you want to restore and click the **Restore** to finish the restore.	**Tools > Config Restore** 

15.5 Enabling Optional Module

When you have not purchased the product, the default license key in the product are trial license. This means that all the functions are valid for a given period, say 7 days, for you to trial. After that periold, the function will not work anymore but just bypass the in / out traffic. It will not interrupt your network but just disable each function.

After you have decided to purchase the product, your system intetrator will give you a deal license key to make permanent effectiveness of each purchased function.

Step 1 **Enter license** Click the License item to enter the license key.	**Update > License** 

Step 2 **Input License Key** Enter the license key and click the **OK** button.	**Update > License** 
Step 3 **Update license successfully** After you successfully update the license, the dialog will pop up. Click the **OK** button to continue.	

15.6 Upgrading Patterns / URL DB

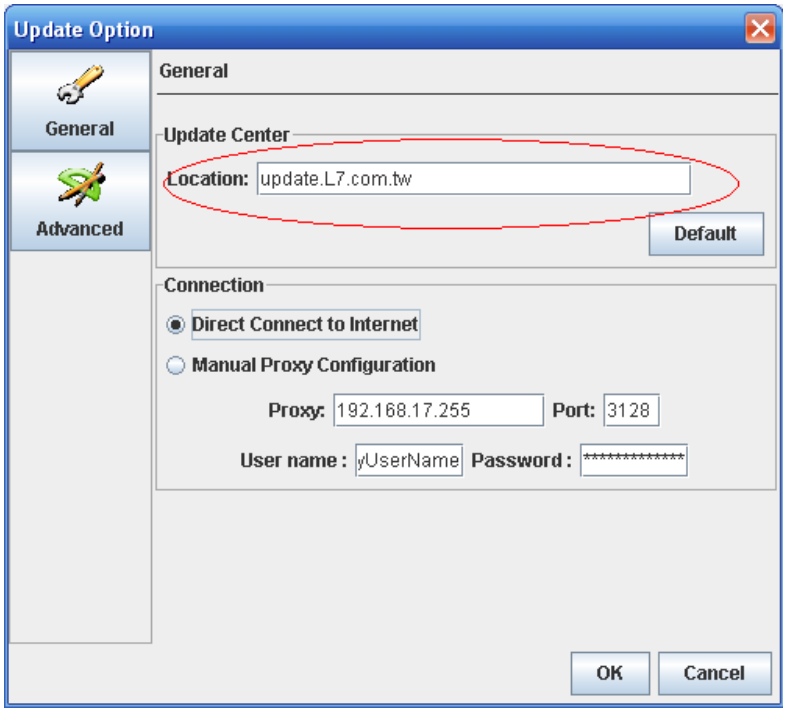
15.6.1 Auto Upgrading Patterns / URLDB

Step 1 **Auto Upgrade Configuration** Click the **Option...**	**Update > Option…** 

Step 2 **Input Update Center Information**

Enter the IP or FQDN of the update center. You can click the default to restore to the default update center. If your company has proxies, click Manual Proxy Configuration and enter the parameters such as IP / port username, password to enable updates through proxies.

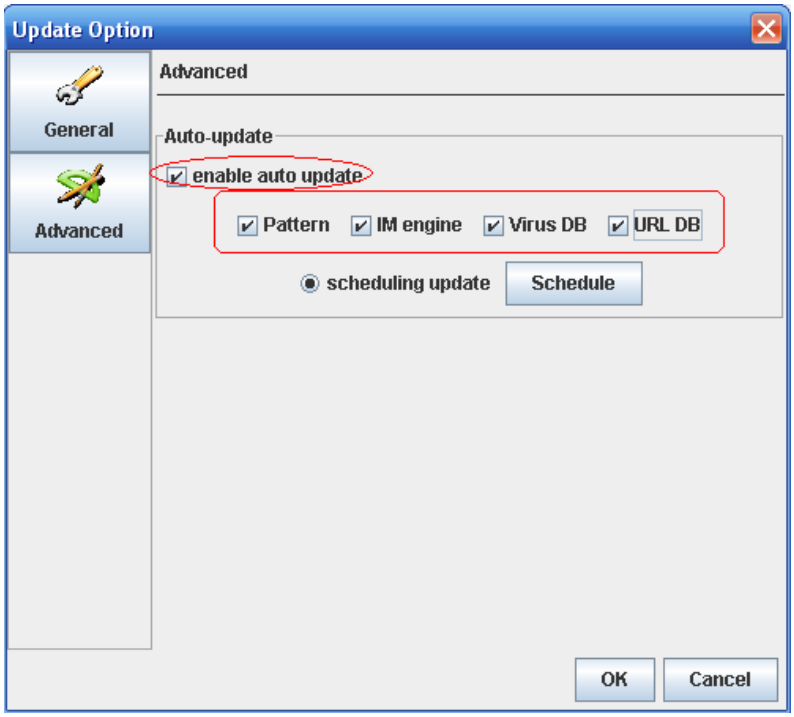
Update > Option… > General

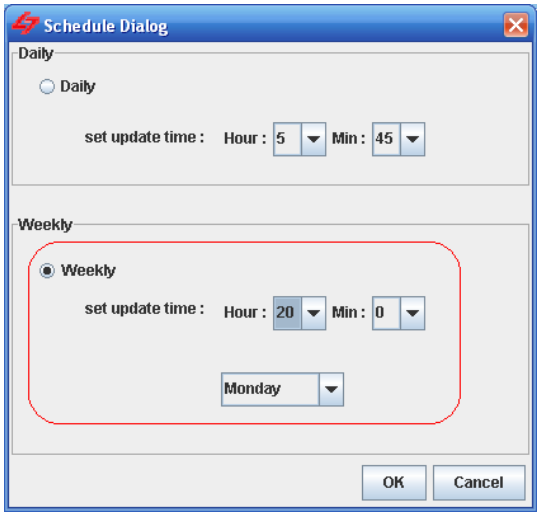


Step 3 **Enable Auto Update**

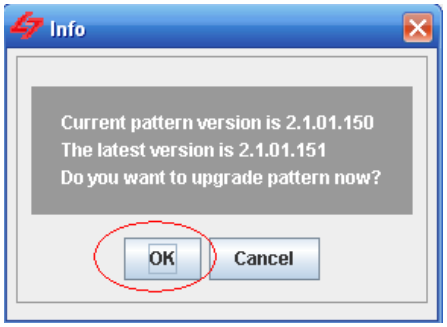
Check the **Enable auto update** and the functions you want to auto update. Click the **Schedule** button to setup the periodical time to upgrade.

Update > Option… > Advanced



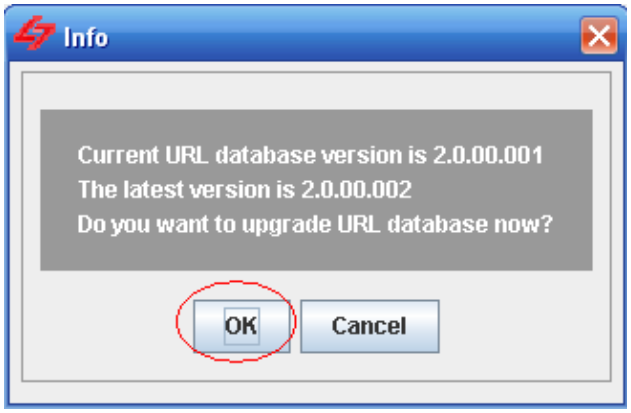
Step 4 **Setup Update Schedule** Select **Weekly** and choose the time you want to update the patterns. Click the the **OK** to finish the settings.	**Update > Option… > Advanced > Schedule** 

15.6.2 Manually Upgrade Application Patterns

Step 1 **Upgrade pattern from UI** Click the **Update pattern**.	**Update > Update pattern** 
Step 2 **Upgrade patterns** Click the OK button to start updating application patterns.	**Update > Update pattern** 

Step 3 **Upgrade patterns from CLI** Enter privileged mode in CLI and then input **sys module update pattern** or **sys module update all** to check for any update.	InstantScan# sys module update all The im-engine version(2.0.02) is the latest one on the device. No upgrade is needed. The pattern version(2.1.01.151) is the latest one on the device. No upgrade is needed. A new version(1.0.00.003) is issued. Please upgrade the newest av-database version to the device. Do you really want to continue upgrade[Y/N]? [N]? y Upgrade av-database from [192.168.17.97]... This process may take a long time, so please be patient.... Successfully update the av-database(new version: 1.0.00.003). A new version(2.0.00.002) is issued. Please upgrade the newest url-database version to the device. Do you really want to continue upgrade[Y/N]? [N]? y Upgrade url-database from [192.168.17.97]... This process may take a long time, so please be patient.... Successfully update the url-database(new version: 2.0.00.002). InstantScan#

15.6.3 Manually Upgrading URLDB

Step 1 **Upgrade URLDB from UI** Click the **Update URL database**.	**Update > Update URL database** 
Step 2 **Upgrading URLDB** Click the **OK** button to start updating the URLDB.	**Update > Update URL database** 
Step 3 **Upgrading URLDB from CLI** Enter privileged mode in CLI and then input **sys module update url** or **sys module update all** to check for any update.	InstantScan# sys module update all The im-engine version(2.0.02) is the latest one on the device. No upgrade is needed. The pattern version(2.1.01.151) is the latest one on the device. No upgrade is needed. A new version(1.0.00.003) is issued. Please upgrade the newest av-database version to the device. Do you really want to continue upgrade[Y/N]? [N]? y Upgrade av-database from [192.168.17.97]... This process may take a long time, so please be patient.... Successfully update the av-database(new version: 1.0.00.003). A new version(2.0.00.002) is issued. Please upgrade the newest url-database version to the device. Do you really want to continue upgrade[Y/N]? [N]? y Upgrade url-database from [192.168.17.97]... This process may take a long time, so please be patient.... Successfully update the url-database(new version: 2.0.00.002). InstantScan#

15.6.4 Restore to Factory Default in CLI

Step 4 **Restore to factory default** In CLI, enter **sys resetconf now**, system will reboot and restore to factory default.	InstantScan> en InstantScan# sys resetconf now Config/Modules reset to default.... Config reset done. System will reboot now Press ctrl+e in 5 secs to start with emergency kernel. Booting. Checking Initial Key of this device.....[OK] InstantScan login: _

15.6.5 Restore to Factory Default in CLI Emergency Mode

Step 1 **Enter boot loader** If your firmware accidentally encounters critical damage and cannot enter normal CLI, your can enter emergency mode to restore the firmware back to factory default. You must press <ctrl+e> during the boot-up countdown 5 seconds.	Press ctrl+e in 5 secs to start with emergency kernel. Enter emergency mode. (Emergency Mode) login as "admin", no password [EMERGENCY] login: admin [EMERGENCY]> en [EMERGENCY]# disable Turn off privileged mode command exit Exit command shell ip Configure/Display IP related settings sys Configure system parameters [EMERGENCY]# sys resetconf now Config reset to default. System will reboot now

15.6.6 SNMP Control

Step 1 Enable SNMP Control Check the **SNMP Control** in the menu.	**Tools > SNMP Control** 
Step 2 Setup SNMP Control After you setup SNMP parameters, you can monitor system and network status from the remote.	**Tools > SNMP Control**

Field	Description	Example
Enable SNMP	Enable SNMP remote monitor	Enable
System name	The name of the device	WALL-1.yourCompany.com
System location	The location of the device	Office
Contact info	The information of the contact person	mis
Get community	This field acts as a password to get the SNMP information	public-ro
Set Community	This field acts as a password to set the SNMP information	private-rw
Trusted host	The host which we trust and allow him to get / set SNMP	192.168.1.5
Trap community	When launching an SNMP trap, use this field as a password	trap-comm
Trap destination	When an SNMP trap occurs, notify this filed as its destination	192.168.1.5

Chapter 16
Advanced Multi-Layer Architecture

This chapter introduces the advanced multi-layer architecture for management

16.1 Scenario

A company should have its architecture. The hierarchy of the architecture includes different divisions to facilitate the responsibility. If the device is used to collect the content of the networks, the data is very sensitive to the hierarchy of the company's architecture. If an IT member who is managing the product has the full permissions to access the recorded contents, it would be very dangerous. If he or she can read the data of another divisioin or the data of his / her boss, the one who is under the management of his / her boss will have larger permission than his / her boss. Actually, auditing belongs to the department of auditing, not the IT member. The system should have a mechanism to separate the data and control of the system.

16.2 Objectives

Since a content recorder is related to personal privacy, the data should be kept confidentially. The product's advanced layered management and auditing mechanism can define multiple accounts with different permissions. Hence, IT member can set policy rules but cannot see the recorded data. Auditing department can only see the recorded data but they cannot set policy rules. Administrators can see all the data and can also control all the policy rules.

16.3 Methodology

Currently the device has 3 permissions, including

1. **Admin:** the most powerful user who can do anything in the device. You should strictly disallow the IT member to own this permission except for the initial stage of the deployment of this device.
2. **MIS:** This level's permission includes the configuration of any policy rules without touching any recorded data or reports.
3. **Audit:** This level's permission includes browsing of chat contents, URL access logs, and reports.

16.4 Steps

When you first login into the product, you can go to the Account Manager to edit the users and passwords that will access the device.

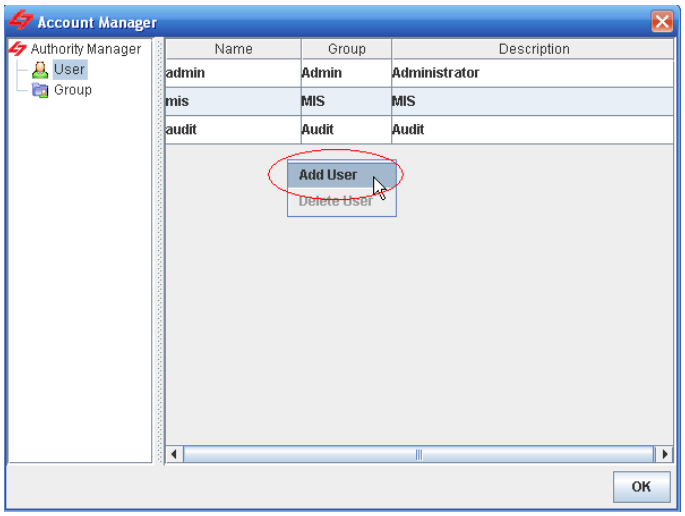
16.4.1 Creating a New User Account

Step 1 Setup user account Click the **Account Manager** item.	**Tool > Account Manager** 

Step 2 Adding new user account

The product allows multiple logins from different people. You can setup the accounts and their corresponding permissions.

Tool > Account Manager > User > Add User



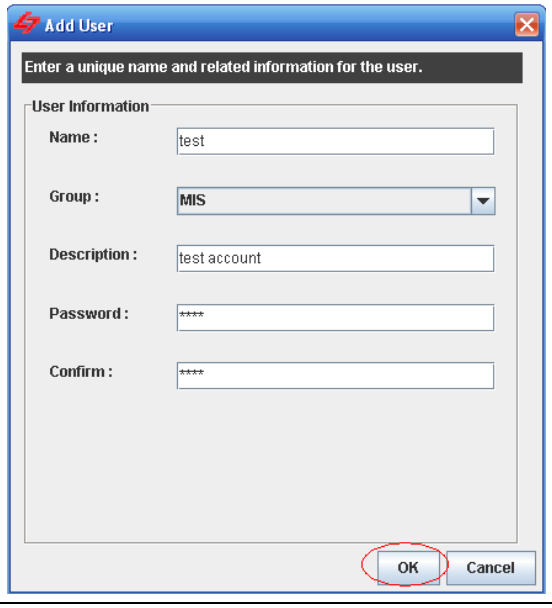
Field	Description	Example
Name	The account name of the user who can enter the system	test
Group	1. **Admin:** the most powerful user who can do anything in the device. You should strictly disallow the IT member to own this permission except for the initial stage of the deployment of this device. 2. **MIS:** This level's permission includes the configuration of any policy rules without touching any recorded data or reports. 3. **Audit:** This level's permission includes browsing of chat contents, URL access logs, and reports.	mis
Description	Detailed description of an account	test account

FIGURE 16-1 Account Manager

Step 3 Edit an account

Input the name of the account and input the description of the account. Enter the password and its confirmation. After that, click the OK button to finish the settings.

Tool > Account Manager > User > Add User



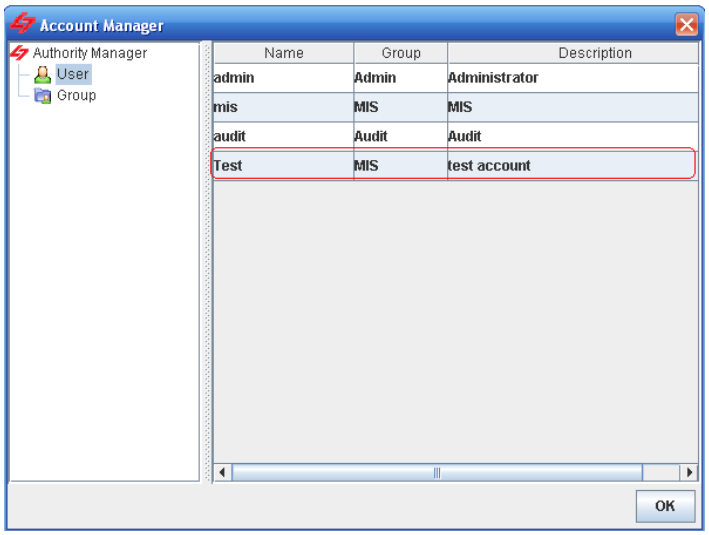
Step 4 Successfully created

When you successfully create an account, you will be notified a dialog as in the right figure. Click the OK button to continue.

Step 5 Display all accounts

After you have finishing adding an account, you can see what you have entered in the **Account Manager** window.

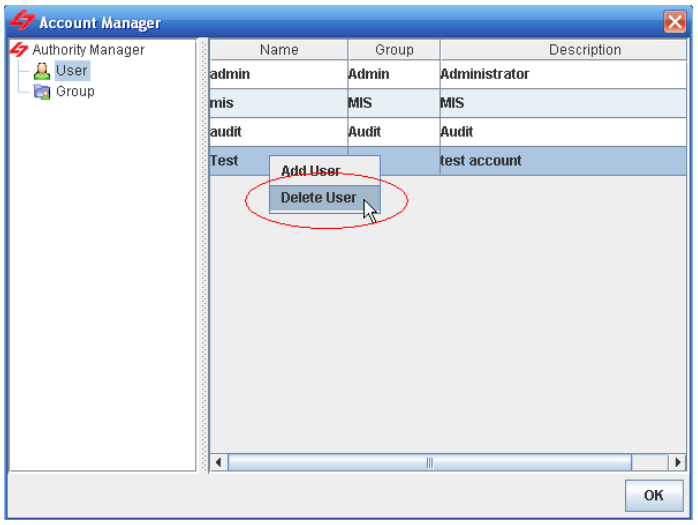
Tool > Account Manager > User



Step 6 Delete an account

If you want to delete an account, you only need to select the **Delete User** item.

Tool > Account Manager > User > Delete User



16.4.2 Modify Passwords

Step 1 Change the passowrd

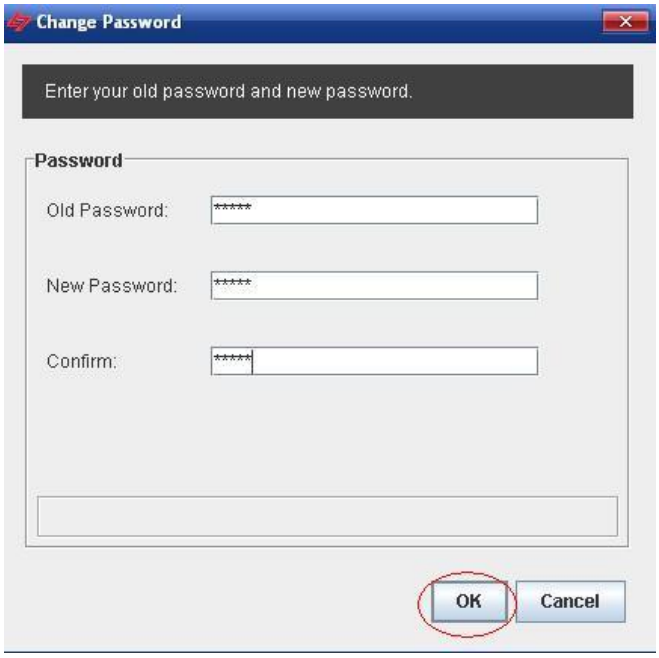
Click the **Change Password** item.

Tool > Change Password

Step 2 Enter new password

Enter the **Old Password** and the **New Password** and enter the new password again in the **Confirm** field. Click the **OK** button to finish the settings.

Tool > Change Password



Appendix

Appendix A
Command Line Interface

You can use Management Client to setup your product. Besides, you can also use console / ssh / telnet to remotely configure or query the device. CLI is necessary when you setup network addresses and the 2/3-tier architecture. It also helps you to reset back to factory defaults or shutting down the system. We arrange all supported CLI commands as follows.

A.1 CLI Commands – Non-Priviledged Mode

When you connect to the product by console/telnet/SSH, you need to use CLI commands to setup the product. The default login user name and password pair is admin / admin.

Non-privileged mode

Main Command	Sub Command	Example	Description
?		?	List all the items
enable (en)		enable	Enable the priviledged mode
exit (ex)		exit	Exit the CLI
ip			IP address setup
	ping	ip ping 202.11.22.33	Diagnose the network by ping
	traceroute	ip traceroute 202.11.22.33	Diagnose the network by traceroute
sys			System settings
	status (st)	sys status	Show the system status
	version (ver)	sys version	Show the firmware / pattern / urldb version

FIGURE A-1 Non-Priviledged Mode

Note: If you don't know the parameters of a command, you can type "?" anytime after your current command. For example, type "ip ?" will list all possible parameters following the ip command.

Privileged mode

Command		Example	Description
?		?	List all the items
disable (dis)		disable	Exit the priviledged mode
exit (ex)		exit	Exit the CLI interface
ip			IP address setup
	ifset	ip ifset INTF1	Display or set the interface negotiation mode
	ping	ip ping 202.11.22.33	Sending ICMP for network debugging
	set	ip set	Setting up network addresses
	show	ip show	Display all network settings
	tftp (upgrade)	ip tftp upgrade image <FILENAME> 192.168.168.170.	Upgrade firmware by the tftp protocol
	traceroute	ip traceroute 202.11.22.33	Tracing the routes for network debugging
sys			Setting up system parameters
	date	sys date	Display or configure the system time
	halt	sys halt now	Shutdown the system
	module	sys module	Updating/Restoring module settings
	password	sys password	Changing the system password
	reboot	sys reboot now	Rebooting the system
	resetconf	sys resetconf now	Resetting the configuration
	sessionlog	sys ressionlog on	Turing on/off session logging
	status (st)	sys status	Display the system status
	tcpdump	sys tcpdump management	Dumping passing packets
	version (ver)	sys version	Display system firmware/patter versions

The complete “sys tcpdump” commands are listed as below:

Main	2nd	3rd	last	Example	Description
sys	tcpdump	External	dump	sys tcpdump external dump	Dump external port packets
			interactive	sys tcpdump external interactive	Dump external port packets interactively
		Internal	dump	sys tcpdump internal dump	Dump internal port packes
			interactive	sys tcpdump internal interactive	Dump internal port packets interactively
		Management	dump	sys tcpdump management dump	Dump management port packts

			interactive	sys tcpdump management interactive	Dump management port packets interactively

FIGURE A-6 sys tcpdump

A.2 CLI Commands - Emergency Mode

If the system accidentally crashes and requires you to enter the emergency mode, press Ctrl+e when the prompt shows to you. Enter admin without any password to enter the emergency mode.

Non-privileged mode

Command		Example	Description
?		?	Display all items
enable (en)		Enable	Enter the priviledged mode
exit (ex)		Exit	Exit the CLI interface
ip			Setting up IP address related settings
	ping	ip ping 202.11.22.33	Sending ICMP for network debugging
	traceroute	ip traceroute 202.11.22.33	Tracing the routes for network debugging
sys			System related settings
	date	sys date	Display the current time

FIGURE A-7Non-Priviledged Mode in Emergency CLI

Privileged mode

Command		Example	Description
?		?	Display all items
disable (dis)		Disable	Exit from the priviledged mode
exit (ex)		Exit	Exit the CLI interface
ip			Setting up IP related configuration
	ping	ip ping 202.11.22.33	Sending ICMP for network debugging
	set	ip set	Setting up IP address for the devices
	show	ip show	Display all the IP-related settings
	tftp (upgrade)	ip tftp upgrade image <FILENAME> 192.168.168.170.	Upgrade firmware from the TFTP server
	traceroute	ip traceroute 202.11.22.33	Tracing the routes for network debugging
sys			System settings
	date	sys date	Setting the current time/date.
	halt	sys halt now	Shutdown the system
	reboot	sys reboot now	Rebooting the system
	resetconf	sys resetconf now	Restore settings to factory defaults.
	resetpasswd	sys resetpasswd	Changing the password

	showmac	sys showmac	Display the network MAC addresses

FIGURE A-8 Priviledged mode in Emervency CLI

Appendix B
Troubleshooting

1. Why can't I use MSN or Yahoo Messengers after enabling the IM Manager?

Ans: Since enabling the IM Manager will automatically filters non-standard IM traffic through non-standard ports, your IM traffic may not get through the product.

A. Go to Report->App Policy to check if the logs contain any blocking of MSN.
B. If your organization uses proxies through port 80, you should enable Encapsulation Manager to manage IM traffic over SOCKS / HTTP Proxy. Otherwise, you should manually setup each client PC to not use proxy in their MSN settings.
C. If you don't want to start the Encapsulation Manager, neither changing the settings of each client PC, you should at least open the outbound port 1863 for MSN, or 5050 for Yahoo Messenger, or 5190 for AOL / ICQ in your firewall settings.

2. How to upgrade the firmware?

Ans: Contact your dealers to get the newest firmware. Enter the command "ip tftp upgrade image filename.bin x.x.x.x. As for how to setup a tftp server, please check the manual.

3. Why my management server cannot receive any logs?

Ans: Please follow the steps below to check

Step 1. Have you config "sys mgtserver" in CLI to explicit tell the device where to send the logs?
Step 2. Is there any personal firewall or antivirus system installed in your management server? If yes, turn it off.
Step 3. Open 4 ports in your personal firewall: TCP/80, TCP/1080, TCP/3306, and UDP/514.
Step 4. Check if the LogServer service has been started.

4. Why can't I see anything at the console?

Ans:

Please make sure that the baud rate and parameters are 115200, 8, N, 1.

Appendix C
Syslog Format

System Log Format

Product: time=2005-01-10 12:57:27; mod=SYS; sev=<1|2|3|4|5>; tier=<TIER>; lid=<LID>; msg=<Message>; by=<user|system>; from=<IP|console|system>;

Severity	*Level name*
1	Alert
2	Critical
3	Warning
4	Notification
5	Information

TIER	*LID*	*Message*	*Severity*
Client tier=1	A01	Login success	Information
	A01	Login fail, miss password	Information
	A02	Change password	Information
	A04	A new user <user> has been added	Notification
	A05	User <user> has been deleted.	Notification
	A07	Login user <user> login failed due to invalid user name	Information
	S25	Backup configuration file by admin	Warning
	S26	Restore configuration file by admin	Warning
	S27	Download configuration	Warning
	S28	Upload configuration	Warning
Mgtsvr tier=2	L01	Database is full	Critical
	L02	Database is cleanup	Critical
	L03	Backup database to 192.168.17.130	Warning
	L04	Send report to user@yourCompany.com	Information
	L05	Restore database from 192.168.1.1	Warning
	L06	Send alert to user@yourCompany.com	Information
	M01	Change E-Mail Alert setting	Notification
	M02	Change FTP Backup setting	Notification
	M03	Change Report Center setting	Notification
	M04	Change Syslog setting	Notification
sDevice tier=3z	A03	Login success	Information
	A03	Login fail, miss password	Information

	A06	Change password	Information
	S01	Device Startup	Warning
	S02	Device Reboot	Critical
	S03	MGT set to192.168.17.114	Notification
	S04	Gateway IP set to 192.168.17.254	Notification
	S05	Primary DNS set to 10.1.1.1	Notification
	S06	Secondary DNS set to 168.95.1.1	Notification
	S07	Management server set to 192.168.17.112	Notification
	S08	System time updated to 2005-09-04 12:00:00	Notification
	S09	Factory reset to default settings	Warning
	S10	Firmware upgraded to version X.X.XX	Warning
	S10	Firmware upgrade has failed	Critical
	S11	App Policy pattern updated to version X.X.XX.XXX	Warning
	S11	App Policy pattern update has failed	Critical
	S12	IM signature updated to version X.X.XX.XXX	Warning
	S12	IM signature update has failed	Critical
	S13	AVDB updated to version X.X.XX.XXX	Warning
	S13	AVDB update has failed	Critical
	S14	Enable App Policy	Notification
	S14	Disable App Policy	Notification
	S15	Enable IM Manager	Notification
	S15	Disable IM Manager	Notification
	S16	Enable Traffic Manager	Notification
	S16	Disable Traffic Manager	Notification
	S17	Enable HA	Critical
	S17	Disable HA	Critical
	S18	HA mode changed to AA	Critical
	S18	HA mode changed to AS	Critical
	S19	HA type changed to master	Critical
	S19	HA type changed to slave	Critical
	S20	HA monitored node <node_name> failed	Warning
	S21	HA control changed to master	Alert
	S21	HA control changed to slave	Alert
	S22	HA Virtual IP Address: 192.168.17.100	Notification
	S23	HA In-Ping-Nodes: 192.168.17.111	Notification
	S24	HA Ex-Ping-Nodes: 192.168.17.254	Notificaiton
	S29	URLDB	

	S31	App Policy pattern updated to version X.X.XX.XXX	Warning
	S31	App Policy pattern update has failed(error code:XX)	Critical
	S32	reserved for future using	
	S33	AVDB updated to version X.X.XX.XXX	Warning
	S33	AVDB update has failed(error code:XX)	Critical
	S34	URLDB updated to version X.X.XX.XXX	Warning
	S34	URLDB update has failed(error code:XX)	Critical
	S35	IM engine updated to version X.X.XX	Warning
	S35	IM engine has failed(error code:XX)	Critical
	S36	App Policy engine updated to version X.X.XX	Warning
	S36	App Policy engine update has failed(error code:XX)	Critical
	S37	reserved for future using	
	S38	Antivirus database engine updated to version X.X.XX	Warning
	S38	Antivirus database engine update has failed(error code:XX)	Critical
	S39	URL database engine updated to version X.X.XX.XXX	Warning
	S39	URL database engine update has failed(error code:XX)	Critical
	S40	reserved for future using	
	S41	App Policy pattern restored to version X.X.XX.XXX	Warning
	S41	App Policy pattern restore has failed(error code:XX)	Critical
	S42	reserved for future using	
	S43	AVDB restored to version X.X.XX.XXX	Warning
	S43	AVDB restore has failed(error code:XX)	Critical
	S44	URLDB restored to version X.X.XX.XXX	Warning
	S44	URLDB restore has failed(error code:XX)	Critical
	S45	IM engine restored to version X.X.XX.XXX	Warning
	S45	IM engine restore has failed(error code:XX)	Critical
	S46	App Policy engine restored to version X.X.XX	Warning
	S46	App Policy engine restore has failed(error code:XX)	Critical
	S47	reserved for future using	
	S48	Antivirus database engine restored to version X.X.XX	Warning
	S48	Antivirus database engine restore has failed(error code:XX)	Critical
	S49	URL database engine restored to version X.X.XX	Warning
	S49	URL database engine restore has failed(error code:XX)	Critical
	S50	reserved for future using	
	S51	$SWID (Update Successfully. Update database and then respond a new SWID.)	
	S52	$SWID	

		(Keep old license. Don't need to update database and then respond the old SWID.)	
	S53	Request is rejected	
	S54	Invalid HWID	
	S55	This device is not registered	
	S56	This license is invalid	
	S57	This license has been registered	
	S58	This license cannot be used on this device	
	S59	Can not connect to database	
	S60	No such device	
	S61	Can not connect to device	
	S62	Unable to clear database Figure	
	S63	Filter List error	
	S64	Post parameters error	
	S65	Post value is invalid	
	S66	Invalid software ID	
	S67	Execute SQL command fail	
	S68	No version obtained	
	S69	No such database	
	S70	Backup database fail	
	S71	Restore database fail	
	S72	Unmatched pattern version	
	S73	Software ID was reset to trial version	
	S74	Invalid checksum	
	S75	Can not find backup SQL scheme	
	S76	Enable Web Manager	Notification
	S76	Disable Web Manager	Notification

FIGURE D-1 ID for each system log